

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Masato YAMAMICHI et al. :  
Serial No. NEW : **Attn: APPLICATION BRANCH**  
Filed October 8, 2003 : Attorney Docket No. 2003\_1411A  
ENCRYPTION APPARATUS, DECRYPTION  
APPARATUS AND ENCRYPTION SYSTEM :  
THE COMMISSIONER IS AUTHORIZED  
TO CHARGE ANY DEFICIENCY IN THE  
FEES FOR THIS PAPER TO DEPOSIT  
ACCOUNT NO. 23-0975

**CLAIM OF PRIORITY UNDER 35 USC 119**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-296219, filed October 9, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masato YAMAMICHI et al.

By *Michael S. Huppert*  
Michael S. Huppert  
Registration No. 40,268  
Attorney for Applicants

MSH/kjf  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
October 8, 2003

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2002年10月 9日

出願番号

Application Number: 特願2002-296219

[ ST.10/C ]:

[ JP2002-296219 ]

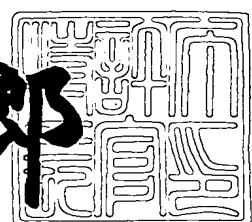
出願人

Applicant(s): 松下電器産業株式会社

2003年 6月 5日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3043722

【書類名】 特許願  
【整理番号】 2022540381  
【提出日】 平成14年10月 9日  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 5/00  
【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内  
【氏名】 山道 将人  
【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内  
【氏名】 布田 裕一  
【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内  
【氏名】 大森 基司  
【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内  
【氏名】 館林 誠  
【特許出願人】  
【識別番号】 000005821  
【氏名又は名称】 松下電器産業株式会社  
【代理人】  
【識別番号】 100097445  
【弁理士】  
【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 暗号システム、送信装置及び受信装置

【特許請求の範囲】

【請求項1】外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置であって、

前記受信装置毎に乱数パラメータを記憶する記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする、送信装置。

【請求項2】前記暗号手段は、NTRU暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする、請求項1に記載の送信装置。

【請求項3】前記制御手段は、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項1または請求項2に記載の送信装置。

【請求項4】前記制御手段は、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする、請求項1または請求項2に記載の送信装置。

【請求項5】外部から暗号文を受信し、復号鍵で復号する受信装置であって、

前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段と、

前記復号文が正しく得られたかどうかを判別する判別手段と、

前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする、受信装置。

【請求項6】外部から入力された平文を暗号化した暗号文を送信する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、

前記送信装置は、

乱数パラメータを記憶するパラメータ記憶手段と、

前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、

前記暗号文を送信する送信手段と、

前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、  
前記受信装置は、

前記暗号文を受信する受信手段と、

前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする  
、暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報セキュリティ技術としての暗号技術に関し、特に、同じ復号鍵を使用し続けると暗号化通信が徐々に復号できなくなっていく暗号システムに関するものである。

【0002】

【従来の技術】

送信装置と受信装置との間で秘匿通信を実現する方法として、公開鍵暗号を用いた暗号化通信がある。簡単に説明すると、送信装置が、通信内容を受信装置の公開鍵を用いて暗号化して送信し、受信装置は、暗号化された通信内容を受信し、それを自身の秘密鍵を用いて復号して元の通信内容を得る方法である（例えば、非特許文献1参照。）。

【0003】

この方法を用いる一般的な暗号システムでは、送信装置及び受信装置は、ともに複数存在する。まず、送信装置は、通信先受信装置の公開鍵を取得する。この公開鍵は、通信先受信装置が有する秘密鍵と対になるものでありシステムにおいて公開されている。そして、送信装置は、通信すべきデータを上記のように取得した公開鍵で暗号化して送信する。一方で、受信装置は、上記のように暗号化された通信データを受信する。そして、受信装置は、暗号化された通信データを、自身の有する秘密鍵で復号して元の通信データを得る。

**【0004】**

ここで、もしも通信先受信装置の有する秘密鍵が暴露されると、上記の暗号システムは、もはや安全ではなくなる。通信先受信装置の公開鍵で暗号化された通信内容は、暴露された秘密鍵をもつ第三者の受信装置でも復号されてしまうからである。従って、受信装置の有する秘密鍵は、外部に露見しないように厳重に管理する必要がある。

**【0005】**

しかしながら、場合によっては、何らかの事故や事件により受信装置の有する秘密鍵が暴露されてしまう可能性がある。従って、上記の暗号システムにおいては、受信装置の有する秘密鍵が暴露された場合、もしくはその疑いがある場合には、暴露された秘密鍵と対になる公開鍵の使用を停止する必要がある。

**【0006】**

そのような方法の例として、証明書廃棄リスト (Certificate Revocation List、CRL) と呼ばれるデータ構造を使用して、受信装置の有する秘密鍵が暴露された場合に、暴露された秘密鍵と対になる公開鍵の使用を停止する方法が開示されている（例えば、非特許文献2参照。）。

**【0007】**

また、他の例として、IEEE (Institute of Electrical and Electronics Engineers) 1394規格によるシリアルバス上を伝送されるデジタルコンテンツを保護するDTC defense (Digital Transmission Content Protection) 規格の中では、SRM (System Renewability Messages) を使用して、受信装置の有する秘密鍵が暴露された場合に、当該受信装置の公開鍵の使用を停止するようになっている（例えば、非特許文献3参照。）。

**【0008】**

以下に、これらの方法を簡単に説明する。

**【0009】**

まず、公開鍵は、それを保有する人や物などの識別情報に関連付けられ、信頼

できる第三者機関によりシリアル番号等が付加された形式に変換される。さらに他者による改ざんを防止するためにその第三者機関のデジタル署名を付加する。これを公開鍵証明書と呼ぶ。そして、第三者機関により発行されるCRLやSRMには、秘密鍵の暴露等の理由で使用を停止すべき公開鍵証明書のシリアル番号が記載されている。よって、CRLやSRMに記載されたシリアル番号をチェックすることにより、暴露された秘密鍵と対になる公開鍵の使用を停止することができる。

#### 【0010】

この方法を、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵証明書のデジタル署名を確認し、その公開鍵証明書から、公開鍵とシリアル番号を取得し、第三者機関から発行されるCRLやSRMを取得する。そして、送信装置は、取得した公開鍵証明書のシリアル番号がCRLやSRMに記載されていれば、その公開鍵の使用を停止する。このことにより、受信装置の有する秘密鍵が暴露されている場合、暴露された秘密鍵と対になる公開鍵の使用を停止することできる。よって、これにより、送信装置と受信装置の間で安全な暗号化通信を実現することができる。

#### 【0011】

##### 【非特許文献1】

岡本龍明、山本博資、「現代暗号」、シリーズ／情報科学の数学、産業図書、1997

##### 【非特許文献2】

山田信一郎 訳、「ディジタル署名と暗号技術」、株式会社ピアソン・エデュケーション、p. 159～p. 214、1997

##### 【非特許文献3】

Digital Transmission Content Protection Specification Revision 1.2 (Informational Version)、[online]、2001年7月11日、[2002年9月13日検索]、インターネット<URL: http://www.dtcp.com/data/info\_dtcp\_v1\_1

2\_20010711.pdf>

【0012】

【発明が解決しようとする課題】

しかし、CRLやSRMを用いた上記方法では、以下のような課題がある。

【0013】

(1) 送信装置が最新のCRLやSRMを取得できない場合、受信装置の有する秘密鍵が暴露されても、送信装置は必ずしも当該受信装置の公開鍵の使用を停止できない。これにより、従来の技術では、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

【0014】

(2) 暗号化通信の安全性確保のためには、鍵を定期的に更新することが望ましい。しかし、従来の技術では、鍵を定期的に更新しなくとも受信装置は正常に動作するため、受信装置を扱う人に、鍵の更新を促しにくい。

【0015】

(3) 信頼できる第三者機関によるCRLやSRMが必要である。

【0016】

以下に、上記問題点(1)、(2)、(3)について詳細を説明する。

【0017】

まず、CRLやSRMを用いた上記方法では、送信装置が最新のCRLやSRMを取得できず、受信装置の有する秘密鍵が暴露されても、当該受信装置の公開鍵の使用を停止できない場合がある。例えば、デジタル化された映画コンテンツデータがDVDなどの記録媒体に記録されるシステムであって、映画コンテンツデータは受信装置に相当するプレーヤ毎の暗号鍵で暗号化されてディスクに記録され、プレーヤはこの暗号鍵に対応する復号鍵を有しており、ディスクに記録されている暗号化映画コンテンツデータを復号して、映画を再生するものであり、さらに特定のプレーヤは不正な機器であって再生を防止する目的で、そのプレーヤの公開鍵のCRLやSRMがDVD等の記憶媒体に記録されて発行されるような場合である。

**【0018】**

いま、ある受信装置の秘密鍵が暴露したことが判明したとする。それ以降は、当該受信装置の公開鍵証明書のシリアル番号が追加記載された最新のCRLやSRMは、DVDに記録されて発行されるが、それ以前に配布されたDVDには古いCRLやSRMが記録されたままである。結果として、古いDVDを用いていると、古いCRLやSRMしか取得できず、必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。

**【0019】**

また、SRMを用いるDTCP規格では、IEEE1394シリアルバスで接続された機器間で、機器が持つ古いSRMは他の機器が持つ新しいSRMに更新されていく。すなわち、この仕組みによって、DVD等の記憶媒体から新しいSRMを取得する以外にも、他の機器からも新しいSRMを取得できる。しかしながら、この仕組みを用いても、完全には最新のSRMを取得できる保証は無い。結果として、送信装置は必ずしも当該受信装置の公開鍵の使用を停止する効果が得られない。従って、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続ける恐れがある。

**【0020】**

次に、CRLやSRMを用いた上記方法では、受信装置を扱う人に、自身の公開鍵・秘密鍵の更新を促しにくい。これは、送信装置が、CRLやSRMにより受信装置の公開鍵の使用を停止するまでは、受信装置は、完全に暗号化通信を復号し続けることが可能であることに起因する。以下にこのことを説明する。

**【0021】**

従来の技術では、暴露された秘密鍵と対になる公開鍵の使用を停止するためには、最新のCRLやSRMを第三者機関のサーバ等から取得して、CRLやSRMに記載されたシリアル番号をチェックしなければならない。しかし、一般に、送信装置を扱う人は、CRLやSRMのチェックを知らずに暗号化通信を行ったり、あるいはサーバ等から最新のCRLやSRMを取得するのが面倒なために、このチェックを無視して暗号化通信を行ったりすることが多い。これは、送信装置が受信装置の公開鍵を取得していれば、CRLやSRMのチェックを行わなく

とも、送信装置、受信装置共に正常に動作して、暗号化通信を行うことができるからである。そして、送信装置がCRLやSRMのチェックを行わないで暗号化通信を行うと、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を更新しようとはしない。なお、公開鍵証明書に有効期限を設け、送信装置が有効期限の切れた公開鍵の使用を停止し、受信装置が鍵を更新しない限り、送信装置から受信装置への暗号化通信を行わないようにする方法もある。しかしながら、この場合も、CRLやSRMを用いる方法と同様に、送信装置を扱う人は有効期限のチェックを知らずに、あるいはこのチェックを無視して暗号化通信を行うことが多い。この結果、CRLやSRMを用いる方法と同様に、鍵を定期的に更新しなくても受信装置が正常に動作するため、受信装置を扱う人は、自身の公開鍵・秘密鍵を定期的に更新しようとはしない。

#### 【0022】

最後に、CRLやSRMを用いた上記方法では、信頼できる第三者機関によるCRLやSRMが前提となっている。これは、信頼できる第三者機関によるCRLやSRMの存在を仮定しなければならない点が問題点である。

#### 【0023】

そこで、本発明は上記（1）、（2）、（3）の課題に鑑み、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第1の目的とする。

#### 【0024】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、同じ秘密鍵を使い続けると、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることを第2の目的とする。

#### 【0025】

また、送信装置が暗号化通信を行うに際して、第三者機関によるC R LやS R Mを必要としない暗号システム、送信装置又は受信装置を提供することを第3の目的とする。

#### 【0026】

##### 【課題を解決するための手段】

請求項1における発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

#### 【0027】

請求項2における発明は、請求項1に記載の送信装置が、N T R U暗号方式の暗号アルゴリズムを用いて暗号文を生成することを特徴とする。

#### 【0028】

請求項3における発明は、請求項1または請求項2に記載の送信装置において、前記制御手段が、期間が経過するにつれて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

#### 【0029】

請求項4における発明は、請求項1または請求項2に記載の送信装置において、前記制御手段が、前記暗号手段の暗号化回数に応じて前記記憶手段に記憶された乱数パラメータを変化させることを特徴とする。

#### 【0030】

請求項5における発明は、外部から暗号文を受信し、復号鍵で復号する受信装置が、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段と、前記復号文が正しく得られたかどうかを判別する判別手段と、前記判別手段の判別結果に応じて前記復号鍵を更新する更新手段とを備えることを特徴とする。

#### 【0031】

請求項6における発明は、外部から入力された平文を暗号化した暗号文を送信

する送信装置、及び前記暗号文を受信して復号する受信装置から構成される暗号システムであって、前記送信装置は、乱数パラメータを記憶するパラメータ記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記暗号文を送信する送信手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備え、前記受信装置は、前記暗号文を受信する受信手段と、前記暗号文を復号して復号文を生成する復号手段とを備えることを特徴とする。

#### 【0032】

##### 【発明の実施の形態】

以下、本発明に係る暗号システムの実施の形態について、図面を用いて説明する。

#### 【0033】

本発明に係る暗号システムは、公開鍵暗号方式の一例として、NTRU暗号方式を用いる。NTRU暗号方式は、多項式の演算で暗号化と復号化を行う公開鍵暗号方式である。このNTRU暗号方式、及びNTRU暗号方式の公開鍵、及び秘密鍵の生成方法については、Jeffery Hoffstein, Jill Pipher, and Joseph H. Silverman, 「NTRU: A ring based public key cryptosystem」, Lecture Notes in Computer Science, 1423, pp. 267-288, Springer-Verlag, 1998. に詳しく述べられているので、ここでは詳細な説明を省略するが、以下にNTRU暗号方式について簡単に説明する。

#### 【0034】

NTRU暗号方式は、整数のシステムパラメータ、 $N$ 、 $p$ 、 $q$ を持つ。上記文献には、システムパラメータの例として、 $(N, p, q) = (107, 3, 64)$ 、 $(N, p, q) = (167, 3, 128)$ 、 $(N, p, q) = (503, 3, 256)$ の3つの例が挙げられている。

#### 【0035】

以降、本発明に係る暗号システムの実施の形態では、システムパラメータ $N$ を

$N = 167$ とした場合の説明を行う。

### 【0036】

NTRU暗号方式は、多項式の演算により暗号化と復号化を行う公開鍵暗号方式である。まず、NTRU暗号方式で扱う多項式は、上記システムパラメータ $N$ に対し、 $N - 1$ 次元以下の多項式であり、例えば $N = 5$ のとき、 $X^4 + X^3 + 1$ 等の多項式である。ここで、「 $X^a$ 」は $X$ の $a$ 乗を意味することとする。また、暗号化時あるいは復号化時に用いる、公開鍵 $h$ 、秘密鍵 $f$ 、平文 $m$ 、乱数 $r$ 、暗号文 $c$ はいずれも、 $N - 1$ 次元以下の多項式として表現される（以降、それぞれを公開鍵多項式 $h$ 、秘密鍵多項式 $f$ 、平文多項式 $m$ 、乱数多項式 $r$ 、暗号文多項式 $c$ と呼ぶ）。

### 【0037】

そして、多項式演算は、上記システムパラメータ $N$ に対し、 $X^N = 1$ という関係式を用いて、演算結果が常に $N - 1$ 次元以下の多項式になるように演算される。例えば、 $N = 5$ の場合、多項式 $X^4 + X^2 + 1$ と多項式 $X^3 + X$ の積は、多項式と多項式の積を $\times$ 、整数と多項式の積を $\cdot$ とすると、 $X^5 = 1$ という関係から、

$$\begin{aligned} & (X^4 + X^2 + 1) \times (X^3 + X) \\ &= X^7 + 2 \cdot X^5 + 2 \cdot X^3 + X \\ &= X^2 \times 1 + 2 \cdot 1 + 2 \cdot X^3 + X \\ &= 2 \cdot X^3 + X^2 + X + 2 \end{aligned}$$

というように、常に $N - 1$ 次元以下の多項式になるように演算される。

### 【0038】

暗号化時には、以下に述べる乱数多項式 $r$ と公開鍵多項式 $h$ とを用いて、平文多項式 $m$ に多項式演算である暗号化アルゴリズム $E$ を施して、暗号文多項式 $c = E(m, r, h)$ を生成する。ここで、 $E(m, r, h)$ は、NTRU暗号方式の暗号化アルゴリズム $E$ に、平文多項式 $m$ 、乱数多項式 $r$ 及び公開鍵多項式 $h$ を入力して得られる多項式演算の結果である。暗号化アルゴリズム $E$ については上記文献に詳しく述べられており、ここでは説明を省略する。

### 【0039】

なお、NTRU暗号方式では、乱数多項式  $r$  を生成するためのパラメータ  $d$  が予め決められており、乱数多項式  $r$  は、 $d$  個の係数が 1 であり、かつ  $d$  個の係数が -1 であり、かつ他の係数は 0 となるように選ぶ。すなわち、乱数多項式  $r$  は  $N - 1$  次元以下の多項式であり、0 次元（定数項）から  $N - 1$  次元まで、 $N$  個の係数があるが、この  $N$  個の係数のうち、 $d$  個の係数が 1 であり、かつ  $d$  個の係数が -1 であり、かつ  $(N - 2d)$  個の係数は 0 となるように選ぶ。上記文献によれば、パラメータ  $N$  が  $N = 167$  の場合、 $d = 18$  である。すなわち、18 個の係数が 1 であり、かつ 18 個の係数が -1 であり、 $131 (= 167 - 36)$  個の係数が 0 となるように乱数多項式  $r$  を選ぶ。

## 【0040】

復号化時には、秘密鍵多項式  $f$  を用いて、暗号文多項式  $c$  に多項式演算である復号アルゴリズム  $D$  を施して、復号文多項式  $m' = D(c, f)$  を生成する。ここで、 $D(c, f)$  は、NTRU暗号方式の復号アルゴリズム  $D$  に、暗号文多項式  $c$ 、及び秘密鍵多項式  $f$  を入力して得られる多項式演算の結果である。復号アルゴリズム  $D$  については上記文献に詳しく述べられており、ここでは説明を省略する。

## 【0041】

ところで、このNTRU暗号方式は、復号文多項式  $m'$  が平文多項式  $m$  と異なる場合が発生する。この場合は、復号時に正しく平文多項式  $m$  が得られないことになる。このことを復号エラーが発生するという。復号エラーは、乱数多項式  $r$ 、平文多項式  $m$ 、公開鍵多項式  $h$ 、秘密鍵多項式  $f$  の組み合わせにより、発生するかどうかが決まる。具体的には、公開鍵多項式  $h$  は、秘密鍵多項式  $f$  とランダム多項式  $g$  との演算結果により生成されるが、この公開鍵多項式  $h$  を生成したときに用いたランダム多項式  $g$ 、乱数多項式  $r$ 、平文多項式  $m$ 、秘密鍵多項式  $f$  の演算結果の多項式 ( $p \cdot r \times g + f \times m$ ) の係数の値が  $-q/2$  から  $q/2$  の間に入らなかったとき、復号エラーが発生する。この復号エラーの発生を完全に避ける手法は現在知られていないが、上記文献によれば、 $N = 167$  の場合、 $d = 18$  とすれば、確率的にほとんど復号エラーは発生せず、実用上問題ないことが明記されている。

## 【0042】

## (実施の形態1)

本発明の実施の形態1における暗号システム1の全体構成を図1に示す。この暗号システム1は平文多項式mの暗号化通信を行うシステムであり、送信装置110と複数の受信装置120a、120b、120cとから構成され、送信装置110と受信装置120a、120b、120cとは通信路130を介して接続されている。

## 【0043】

以下に、送信装置110は複数の受信装置のうち受信装置120aと暗号化通信を行うとし、これらの構成要素について詳細に説明を行う。

## 【0044】

送信装置110は、図2に示すように、平文入力部111、パラメータ記憶部112、タイマ部113、パラメータ制御部114、乱数生成部115、暗号化部116、送信部117及び鍵更新部118から構成される。

## 【0045】

平文入力部111は、外部より入力された平文多項式mを暗号化部116に出力する。

## 【0046】

パラメータ記憶部112は、図3に示すように、受信装置120aの固有番号IDa、公開鍵多項式ha及び乱数パラメータdaを、一組のデータDTa = (IDa, ha, da)として記憶している(受信装置120b、120cについても同様にDTb = (IDb, hb, db)、DTc = (IDc, hc, dc)を記憶している)。ここで、乱数パラメータdaは、暗号化時に用いる乱数多項式rを生成するためのパラメータであり、乱数多項式rの係数のうち、係数が1であるものの数、及び係数が-1であるものの数である。なお、乱数パラメータdaの初期値は、da = 18とする。

## 【0047】

タイマ部113は、一日毎に時間信号を発生し、パラメータ制御部114に入力する。

## 【0048】

パラメータ制御部114は、タイマ部113から時間信号を受け取ったら、パラメータ記憶部112に記憶された乱数パラメータd aの値を1ずつ増加させる（乱数パラメータd b、d cの値も、同様に1ずつ増加させる）。

## 【0049】

乱数生成部115は、パラメータ記憶部112から受信装置120aの乱数パラメータd aを読み出す。そして、読み出した乱数パラメータd aに基づき、d a個の係数が1であり、かつd a個の係数が-1であり、かつその他の係数が0となる乱数多項式rをランダムに生成する。そして、生成した乱数多項式rを暗号化部116へ出力する。

## 【0050】

暗号化部116は、予めNTRU暗号方式の暗号アルゴリズムEを有している。

## 【0051】

暗号化部116は、平文入力部111から平文多項式mを受け取り、パラメータ記憶部112から受信装置120aの公開鍵多項式h aを読み出し、乱数生成部115から乱数多項式rを受け取る。そして、暗号化部116は、乱数多項式rと公開鍵多項式h aを用いて、平文多項式mに前記暗号アルゴリズムEを施して暗号文多項式E(m, r, h a)を生成し、生成した暗号文多項式E(m, r, h a)を送信部117へ出力する。

## 【0052】

送信部117は、暗号文多項式E(m, r, h a)を、通信路130を介して受信装置120aへ送信する。

## 【0053】

鍵更新部118は、通信路130を介して受信装置120a、120b、120cから、固有番号と新たな公開鍵多項式を受信することができる。もしも、受信装置120aの固有番号IDAと公開鍵多項式ha'を受信した場合、鍵更新部118は、パラメータ記憶部112に記憶されているDTa = (IDA, ha, da)を、DTa' = (IDA, ha', da')に更新する。ここでda'

は、乱数パラメータの初期値であり  $d_a' = 18$  である（受信装置 120b、120c から受信した場合は、それぞれ、DTb を DTb'、DTC を DTC' に更新する）。

#### 【0054】

以上に述べた送信装置 110 は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

#### 【0055】

以下に、送信装置 110 の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

#### 【0056】

最初に、送信装置 110 の暗号化通信処理について、図 4 に示すフローチャートを用いて説明する。

#### 【0057】

まず、乱数生成部 115 は、パラメータ記憶部 112 から受信装置 120a の乱数パラメータ  $d_a$  を読み出し（ステップ S101）、そして、読み出した乱数パラメータ  $d_a$  に基づき、 $d_a$  個の係数が 1 であり、かつ  $d_a$  個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式  $r$  をランダムに生成し、生成した乱数多項式  $r$  を暗号化部 116 へ出力する（ステップ S102）。

#### 【0058】

次に、暗号化部 116 は、平文入力部 111 から平文多項式  $m$  を受け取り、パラメータ記憶部 112 から受信装置 120a の公開鍵多項式  $h_a$  を読み出し、乱数生成部 115 から乱数多項式  $r$  を受け取り（ステップ S103）、そして、暗号化部 116 は、乱数多項式  $r$  と公開鍵多項式  $h_a$  を用いて、平文多項式  $m$  に暗号アルゴリズム E を施して暗号文多項式 E ( $m, r, h_a$ ) を生成し、生成した暗号文多項式 E ( $m, r, h_a$ ) を送信部 117 へ出力する（ステップ S104）。

#### 【0059】

次に、送信部 117 は、受け取った暗号文多項式 E ( $m, r, h_a$ ) を、通信

路130を介して受信装置120aへ送信して処理を終了する（ステップS105）。

#### 【0060】

次に、送信装置110の乱数パラメータ更新処理について、図5に示すフローチャートを用いて説明する。

#### 【0061】

まず、パラメータ制御部114は、タイマ部113から時間信号を受け取ったら、ステップS112へ処理を移し、そうでなければ処理を終了する（ステップS111）。

#### 【0062】

そして、パラメータ制御部114は、パラメータ記憶部112に記憶された乱数パラメータdaの値を1ずつ増加させて（乱数パラメータdb、dcの値も、同様に1ずつ増加させる）、処理を終了する（ステップS112）。

#### 【0063】

次に、送信装置110の公開鍵更新処理について、図6に示すフローチャートを用いて説明する。

#### 【0064】

まず、鍵更新部118は、受信装置120a、120b、120cのいずれかから、固有番号と新たな公開鍵を受信したら、ステップS122へ処理を移し、そうでなければ処理を終了する（ステップS121）。

#### 【0065】

そして、鍵更新部118は、パラメータ記憶部112に記憶されているDTa = (IDA, ha, da)を、DTa' = (IDA, ha', da')に更新して処理を終了する（受信装置120aから受信した場合。受信装置120b、120cから受信した場合は、それぞれ、DTbをDTb'、DTcをDTc'に更新する）。ここでda'は、乱数パラメータの初期値でありda' = 18である（ステップS122）。

#### 【0066】

受信装置120aは、図7に示すように、受信部121、秘密鍵記憶部122

、復号化部123、復号文出力部124、鍵再生成部125、及び入力部126から構成される。

## 【0067】

受信部121は、送信装置110から通信路130を介して、暗号文多項式E( $m, r, h_a$ )を受信し、受信した暗号文多項式E( $m, r, h_a$ )を復号化部123へ出力する。

## 【0068】

秘密鍵記憶部122は、受信装置120aの秘密鍵多項式 $f_a$ を記憶している。

## 【0069】

復号化部123は、暗号化部116が有する暗号アルゴリズムEの逆変換である、NTRU暗号方式の復号アルゴリズムDを予め有している。

## 【0070】

復号化部123は、受信部121から暗号文多項式E( $m, r, h_a$ )を受け取り、秘密鍵記憶部122から受信装置120aの秘密鍵多項式 $f_a$ を読み出す。そして、復号化部123は、秘密鍵多項式 $f_a$ を用いて、暗号文多項式E( $m, r, h_a$ )に前記復号アルゴリズムDを施して復号文多項式 $m' = D(E(m, r, h_a), f_a)$ を生成し、生成した復号文多項式 $m'$ を復号文出力部124へ出力する。

## 【0071】

復号文出力部124は、復号化部123から復号文多項式 $m'$ を受け取り、復号文多項式 $m'$ を外部へ出力する。

## 【0072】

鍵再生成部125は、入力部126を介して鍵再生成要求信号を受け取った場合、NTRU暗号の秘密鍵多項式 $f_a'$ 及び公開鍵多項式 $h_a'$ を新たに再生成して、秘密鍵記憶部122に記憶されている秘密鍵多項式 $f_a$ を新たに生成した秘密鍵多項式 $f_a'$ に更新する。そして、受信装置120aの固有番号IDAと新たな公開鍵多項式 $h_a'$ を、通信路130を介して送信装置110に送信する。

## 【0073】

受信装置120aを扱うユーザは、受信装置120aの公開鍵多項式 $h_a$ と秘密鍵多項式 $f_a$ の再生成を指示する鍵再生成要求信号を入力部126に入力することができる。この鍵再生成要求信号は、復号文出力部124から出力された復号文多項式 $m'$ が正しく得られない等の理由で、ユーザが公開鍵多項式 $h_a$ と秘密鍵多項式 $f_a$ の再生成のために入力する信号である。

## 【0074】

入力部126は、外部から入力された鍵再生成要求信号を鍵再生成部125に outputする。

## 【0075】

以上に述べた受信装置120aは、以下に述べる復号化処理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

## 【0076】

以下に、送信装置120aの動作について、復号化処理、鍵更新処理に分けて説明を行う。

## 【0077】

最初に、受信装置120aの復号化処理について、図8に示すフローチャートを用いて説明する。

## 【0078】

まず、受信部121は、送信装置110から通信路130を介して、暗号文多項式 $E(m, r, h_a)$ を受信し、受信した暗号文多項式 $E(m, r, h_a)$ を復号化部123へ出力する（ステップS151）。

## 【0079】

次に、復号化部123は、受信部121から暗号文多項式 $E(m, r, h_a)$ を受け取り、秘密鍵記憶部122から受信装置120aの秘密鍵多項式 $f_a$ を読み出し（ステップS152）、そして、復号化部123は、秘密鍵多項式 $f_a$ を用いて、暗号文多項式 $E(m, r, h_a)$ に復号アルゴリズムDを施して復号文多項式 $m' = D(E(m, r, h_a), f_a)$ を生成し、生成した復号文多項式 $m'$ を復号文出力部124へ出力する（ステップS153）。

## 【0080】

次に、復号文出力部124は、復号化部123から復号文多項式 $m'$ を受け取り、復号文多項式 $m'$ を外部へ出力して処理を終了する（ステップS154）。

## 【0081】

次に、受信装置120aの鍵更新処理について、図9に示すフローチャートを用いて説明する。

## 【0082】

まず、鍵再生成部125は、もしも、入力部126を介して鍵再生成要求信号を受け取ったら、ステップS162へ処理を移し、そうでなければ処理を終了する（ステップS161）。

## 【0083】

そして、鍵再生成部125は、NTRU暗号の秘密鍵多項式 $f_a'$ 及び公開鍵多項式 $h_a'$ を新たに再生成して、秘密鍵記憶部122に記憶されている秘密鍵多項式 $f_a$ を新たに生成した秘密鍵多項式 $f_a'$ に更新し（ステップS162）、受信装置120aの固有番号IDaと新たな公開鍵多項式 $h_a'$ を、通信路130を介して送信装置110に送信して処理を終了する（ステップS163）。

## 【0084】

以下に、実施の形態1における暗号システム1全体の動作について説明する。

## 【0085】

今、暗号システム1において、送信装置110は複数の受信装置のうち受信装置120aと暗号化通信を行うとする。

## 【0086】

まず、送信装置110は、受信装置120aの固有番号IDa、公開鍵多項式 $h_a$ 及び乱数パラメータdaを、データDTa = (IDa, ha, db)としてパラメータ記憶部112に記憶している（受信装置120b、120cについても同様にDTb = (IDb, hb, db), DTc = (IDc, hc, dc)を記憶している）。乱数パラメータda、db、dcの初期値は、da = db = dc = 18である。

## 【0087】

そして、送信装置110は暗号化通信処理に従って、平文多項式mを暗号化して暗号文多項式E(m, r, ha)を生成し、生成した暗号文多項式E(m, r, ha)を通信路130を介して受信装置120aに送信する。一方、受信装置120aは前述した復号化処理に従って、暗号文多項式E(m, r, ha)を通じて通信路130を介して送信装置110から受信し、受信した暗号文多項式E(m, r, ha)を復号して復号文多項式m'を出力する。

## 【0088】

なお、送信装置110では、乱数パラメータ更新処理に従って、タイマ部113が一日毎に発生する時間信号に応じて、パラメータ制御部114は、パラメータ記憶部112に記憶された全ての乱数パラメータda、db、dcの値を1ずつ増加させる。すなわち、パラメータ記憶部112に記憶された全ての乱数パラメータの値は一日毎に増加する。

## 【0089】

従って、この送信装置110の暗号化通信処理が継続して行われると、暗号文多項式E(m, r, ha)を生成される際に用いられる乱数多項式rは、係数が1であるもの、及び係数が-1であるものの数が一日毎に増加する。

## 【0090】

今、図10は、乱数パラメータdの値に対し、d個の係数が1であり、かつd個の係数が-1であり、かつその他の係数が0となる乱数多項式rを用いた場合の、NTRU暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータdaの初期値da=18においては、送信装置110が生成する暗号文多項式E(m, r, ha)は、ほとんど復号エラーは発生しない（受信装置120は受信した暗号文多項式E(m, r, ha)から、平文多項式mと等しい復号文多項式m'を得ることができる）。一方で、期間が経過すれば、乱数パラメータdaが一日毎に徐々に大きくなるので、送信装置110が生成する暗号文多項式E(m, r, ha)は、徐々に復号エラー発生確率が大きくなる（受信装置120は受信した暗号文多項式E(m, r, ha)から、平文多項式mと等しい復号文多項式m'を得ることが徐々にできなくなる）。

## 【0091】

そして、もしも受信装置120が平文多項式mと等しい復号文多項式m'を得る確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置120aを扱うユーザは、鍵更新処理を行うことにより、受信装置120aの公開鍵多項式h<sub>a</sub>と秘密鍵多項式f<sub>a</sub>の再生成を指示する鍵再生成要求信号を入力部126に入力することができる。すると、送信装置110の公開鍵更新処理により、パラメータ記憶部112の乱数パラメータd<sub>a</sub>は初期値d<sub>a'</sub>=18に更新されるので、復号エラー発生確率が元に戻り、再び受信装置120aは実用的に暗号化通信を行うことができるようになる。

## 【0092】

実施の形態1では、送信装置110が暗号化通信時に用いる乱数多項式rを、期間が経過するにつれて、係数が1であるもの、及び係数が-1であるものの数を増加させるようにしている。これにより、受信装置120aの有する秘密鍵多項式f<sub>a</sub>が暴露されたとしても、暴露された秘密鍵多項式f<sub>a</sub>を不正に用いる第三者の受信装置では、期間が経過するにつれて、復号エラーの発生確率が大きくなり、送信装置110が行う暗号化通信を正しく復号できなくなる。この結果、この暗号システム1は、従来技術と異なり、秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することができるようになる。

## 【0093】

また、正規に秘密鍵多項式f<sub>a</sub>を有する受信装置120aにおいても、期間が経過するにつれて、同じ秘密鍵多項式f<sub>a</sub>を使い続けると、徐々に復号エラーの発生確率が大きくなり、送信装置110が行う暗号化通信を正しく復号できなくなる。そして、受信装置120aを扱うユーザに、同じ秘密鍵多項式f<sub>a</sub>を使い続けると、復号エラーの発生確率が大きくなってしまい、鍵を更新しないと暗号化通信が実用にならなくなることを知らしめ、鍵の更新のために受信装置120の入力部126を介して、鍵再生成要求信号を入力することを促すことができる。この結果、この暗号システム1は、従来技術と異なり、受信装置又は受信装置を扱う人に、鍵の更新を促すことができるようになる。

## 【0094】

さらに、この暗号システム1は、従来技術と異なり、第三者機関によるCRLやSRMを必要としない。

#### 【0095】

##### (実施の形態2)

本発明の実施の形態2における暗号システム2は、暗号システム1を基本にして構成した、映画や音楽などのデジタル著作物（以降、コンテンツと呼ぶ）の配信に適した暗号システムである。

#### 【0096】

平文多項式mをNTRU暗号で暗号化して送信する代わりに、デジタルデータであるコンテンツCNT<sub>i</sub>（ $1 \leq i \leq k$ ）を暗号鍵K<sub>i</sub>（ $1 \leq i \leq k$ ）を用いて共通鍵暗号で暗号化し、その暗号鍵K<sub>i</sub>（ $1 \leq i \leq k$ ）をNTRU暗号で暗号化して、暗号化したコンテンツと暗号化した暗号鍵を送信する点が暗号システム1と異なる。また、鍵サーバを利用して鍵の更新を行う点が暗号システム1と異なる。以下に詳細を説明する。

#### 【0097】

実施の形態2における暗号システム2の全体構成を図11に示す。この暗号システム2はコンテンツCNTの配信を行うシステムであり、コンテンツサーバ210と、鍵サーバ220と、受信装置230とから構成され、コンテンツサーバ210と受信装置230はインターネット240を介して接続されており、コンテンツサーバ210と鍵サーバ220は専用回線250で接続されており、鍵サーバ220と受信装置230とは、電話回線260で接続されている。

#### 【0098】

コンテンツサーバ210は、コンテンツCNTをユーザjに提供する業者が有しており、鍵サーバ220は、コンテンツCNTを利用するための復号鍵をユーザjに提供する業者が有しており、受信装置230は、コンテンツCNTを利用するユーザjが有している。

#### 【0099】

以下に、これらの構成要素について詳細に説明を行う。

#### 【0100】

コンテンツサーバ210は、図12に示すように、コンテンツ記憶部211、パラメータ記憶部212、タイマ部213、パラメータ制御部214、乱数生成部215、暗号鍵生成部216、暗号化部217、送信部218及び鍵更新部219から構成される。

#### 【0101】

コンテンツ記憶部211は、外部より入力されたコンテンツCNTを、例えば一定時間毎に区切ったMPEG2データCNT<sub>i</sub> ( $1 \leq i \leq k$ )として格納している。

#### 【0102】

パラメータ記憶部212は、図13に示すように、ユーザj毎に、受信装置230の固有番号ID<sub>j</sub>、公開鍵多項式h<sub>j</sub>及び乱数パラメータd<sub>j</sub>を、一組のデータDT<sub>j</sub> = (ID<sub>j</sub>, h<sub>j</sub>, d<sub>j</sub>) ( $1 \leq j \leq n$ )として記憶している。ここで、乱数パラメータd<sub>j</sub>は、暗号化時に用いる乱数多項式r<sub>i</sub> ( $1 \leq i \leq k$ )を生成するためのパラメータであり、乱数多項式r<sub>i</sub> ( $1 \leq i \leq k$ )の係数のうち、係数が1であるものの数、及び係数が-1であるものの数である。なお、乱数パラメータd<sub>j</sub>の初期値は、d<sub>j</sub> = 18とする。

#### 【0103】

タイマ部213は、一日毎に時間信号を発生し、パラメータ制御部214に入力する。

#### 【0104】

パラメータ制御部214は、タイマ部213から時間信号を受け取ったら、パラメータ記憶部212に記憶されたデータDT<sub>j</sub>の乱数パラメータd<sub>j</sub> ( $1 \leq j \leq n$ )の値を1ずつ増加させる。

#### 【0105】

乱数生成部215は、パラメータ記憶部212から送信装置230の乱数パラメータd<sub>j</sub>を読み出す。そして、読み出した乱数パラメータd<sub>j</sub>に基づき、d<sub>j</sub>個の係数が1であり、かつd<sub>j</sub>個の係数が-1であり、かつその他の係数が0となる乱数多項式r<sub>i</sub> ( $1 \leq i \leq k$ )をランダムに生成する。そして、生成した乱数多項式r<sub>i</sub> ( $1 \leq i \leq k$ )を暗号化部217へ出力する。

## 【0106】

暗号鍵生成部216は、ランダムに暗号鍵 $K_i$  ( $1 \leq i \leq k$ ) を生成し、暗号化部217へ出力する。

## 【0107】

暗号化部217は、予めNTRU暗号方式の暗号アルゴリズムEと、例えばDES暗号方式のような共通鍵暗号アルゴリズムSymを有している。

## 【0108】

共通鍵暗号では、暗号鍵Kを用いて、平文mに共通鍵暗号アルゴリズムSymを施して、暗号文 $c = Sym(m, K)$ を生成し、暗号鍵Kを用いて、暗号文cに共通鍵暗号アルゴリズムSymを施して、復号文 $m' = Sym(c, K)$ を生成する。ここで、暗号文生成時に用いた暗号鍵Kと復号文生成時に用いる暗号鍵Kが同一であれば、 $m' = m$ となる。なお、共通鍵暗号及びDES暗号方式については、非特許文献1に詳しく述べられているため、ここでの詳細な説明は省略する。

## 【0109】

暗号化部217は、暗号鍵生成部216から暗号鍵 $K_i$  ( $1 \leq i \leq k$ ) を受け取り、受け取った暗号鍵 $K_i$  ( $1 \leq i \leq k$ ) をNTRU暗号で暗号化できるように暗号鍵多項式 $KPi$  ( $1 \leq i \leq k$ ) に変換する。この変換は、暗号鍵 $K_i$ をビット列としたとき、例えば、暗号鍵 $K_i$ の下位bビット目の値を $X^b$ の係数として暗号鍵多項式 $KPi$ を構成することで実現できる。すなわち、 $K_i = 10010$  (ビット表現) の場合、 $KPi = X^5 + X^2$ となる。

## 【0110】

そして、暗号化部217は、パラメータ記憶部212から受信装置230の公開鍵多項式 $hj$ を読み出し、乱数生成部215から乱数多項式 $ri$  ( $1 \leq i \leq k$ ) を受け取る。そして、暗号化部217は、乱数多項式 $ri$  ( $1 \leq i \leq k$ ) と公開鍵多項式 $hj$ を用いて、変換した暗号鍵多項式 $KPi$  ( $1 \leq i \leq k$ ) にNTRU暗号方式の暗号アルゴリズムEを施して、暗号化暗号鍵多項式 $EKPi = E(KPi, ri, hj)$  ( $1 \leq i \leq k$ ) を生成する。

## 【0111】

そして、暗号化部217は、コンテンツ記憶部211から、コンテンツCNT<sub>i</sub>（ $1 \leq i \leq k$ ）を受け取り、前記暗号鍵K<sub>i</sub>（ $1 \leq i \leq k$ ）を使用して、コンテンツCNT<sub>i</sub>（ $1 \leq i \leq k$ ）に共通鍵暗号アルゴリズムSymを施して、暗号化コンテンツEC<sub>i</sub>=Sym(CNT<sub>i</sub>, K<sub>i</sub>)（ $1 \leq i \leq k$ ）を生成する。

#### 【0112】

そして、暗号化部217は、暗号化暗号鍵多項式EKPi（ $1 \leq i \leq k$ ）と暗号化コンテンツEC<sub>i</sub>（ $1 \leq i \leq k$ ）を送信部218へ出力する。

#### 【0113】

送信部218は、暗号化暗号鍵多項式EKPi（ $1 \leq i \leq k$ ）と暗号化コンテンツEC<sub>i</sub>（ $1 \leq i \leq k$ ）を、インターネット240を介して受信装置230へ送信する。

#### 【0114】

鍵更新部219は、専用回線250を介して鍵サーバ220から、受信装置230の固有番号IDjと公開鍵多項式hj'（ $1 \leq j \leq n$ ）を受信することができる。もしも、受信装置230の固有番号IDjと公開鍵多項式hj'（ $1 \leq j \leq n$ ）を受信した場合、鍵更新部219は、パラメータ記憶部212に記憶されているデータDTj=（IDj, hj, dj）を、DTj'=（IDj, hj', dj'）に更新する。ここでdj'は、乱数パラメータdjの初期値であり、dj'=18である。

#### 【0115】

以上に述べたコンテンツサーバ210は、以下に述べる暗号化通信処理、乱数パラメータ更新処理及び公開鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

#### 【0116】

以下に、コンテンツサーバ210の動作について、暗号化通信処理、乱数パラメータ更新処理、公開鍵更新処理に分けて説明を行う。

#### 【0117】

最初に、コンテンツサーバ210の暗号化通信処理について、図14に示すフローチャートを用いて説明する。

## 【0118】

まず、乱数生成部215は、パラメータ記憶部212から受信装置230の乱数パラメータ $d_j$ を読み出し（ステップS201）、そして、読み出した乱数パラメータ $d_j$ に基づき、 $d_j$ 個の係数が1であり、かつ $d_j$ 個の係数が-1であり、かつその他の係数が0となる乱数多項式 $r_i$ （ $1 \leq i \leq k$ ）をランダムに生成し、生成した乱数多項式 $r_i$ （ $1 \leq i \leq k$ ）を暗号化部217へ出力する（ステップS202）。

## 【0119】

次に、暗号鍵生成部216は、ランダムに暗号鍵 $K_i$ （ $1 \leq i \leq k$ ）を生成し、生成した暗号鍵 $K_i$ （ $1 \leq i \leq k$ ）を暗号化部217へ出力する（ステップS203）。

## 【0120】

次に、暗号化部217は、暗号鍵生成部216から暗号鍵 $K_i$ （ $1 \leq i \leq k$ ）を受け取り、受け取った暗号鍵 $K_i$ （ $1 \leq i \leq k$ ）をNTRU暗号で暗号化できるように暗号鍵多項式 $K_P i$ （ $1 \leq i \leq k$ ）に変換し（ステップS204）、そして、コンテンツ記憶部211からコンテンツ $CNT_i$ （ $1 \leq i \leq k$ ）を読み出し、パラメータ記憶部212から受信装置230の公開鍵多項式 $h_j$ を読み出し、乱数生成部215から乱数多項式 $r_i$ （ $1 \leq i \leq k$ ）を受け取る（ステップS205）。そして、暗号化部217は、乱数多項式 $r_i$ （ $1 \leq i \leq k$ ）と公開鍵多項式 $h_j$ を用いて、変換した暗号鍵多項式 $K_P i$ （ $1 \leq i \leq k$ ）にNTRU暗号方式の暗号アルゴリズムEを施して、暗号化暗号鍵多項式 $E K_P i = E (K_P i, r_i, h_j)$ （ $1 \leq i \leq k$ ）を生成する（ステップS206）。そして、暗号化部217は、コンテンツ記憶部211から、コンテンツ $CNT_i$ （ $1 \leq i \leq k$ ）を受け取り、前記暗号鍵 $K_i$ （ $1 \leq i \leq k$ ）を使用して、コンテンツ $CNT_i$ （ $1 \leq i \leq k$ ）に共通鍵暗号アルゴリズムSymを施して、暗号化コンテンツ $E C_i = Sym (CNT_i, K_i)$ （ $1 \leq i \leq k$ ）を生成し（ステップS207）、そして、暗号化暗号鍵多項式 $E K_P i$ （ $1 \leq i \leq k$ ）と暗号化コンテンツ $E C_i$ （ $1 \leq i \leq k$ ）を送信部218へ出力する（ステップS208）。

## 【0121】

次に、送信部218は、受け取った暗号化暗号鍵多項式EKP<sub>i</sub>（ $1 \leq i \leq k$ ）と暗号化コンテンツEC<sub>i</sub>（ $1 \leq i \leq k$ ）をインターネット240を介して受信装置230へ送信して処理を終了する（ステップS209）。

## 【0122】

次に、コンテンツサーバ210の乱数パラメータ更新処理について、図15に示すフローチャートを用いて説明する。

## 【0123】

まず、パラメータ制御部214は、タイマ部213から時間信号を受け取ったら、ステップS212へ処理を移し、そうでなければ処理を終了する（ステップS212）。

## 【0124】

そして、パラメータ制御部214は、パラメータ記憶部212に記憶されている乱数パラメータd<sub>j</sub>（ $1 \leq j \leq n$ ）を1ずつ増加させて、処理を終了する（ステップS212）。

## 【0125】

次に、コンテンツサーバ210の公開鍵更新処理について、図16に示すフローチャートを用いて説明する。

## 【0126】

まず、鍵更新部219は、専用回線250を介して鍵サーバ220から、受信装置230の固有番号ID<sub>j</sub>と公開鍵多項式h<sub>j'</sub>（ $1 \leq j \leq n$ ）を受信したら、ステップS222へ処理を移し、そうでなければ処理を終了する（ステップS221）。

## 【0127】

そして、鍵更新部219は、パラメータ記憶部212に記憶されているデータDT<sub>j</sub> = (ID<sub>j</sub>, h<sub>j</sub>, d<sub>j</sub>)を、DT<sub>j'</sub> = (ID<sub>j</sub>, h<sub>j'</sub>, d<sub>j'</sub>)に更新して処理を終了する。ここでd<sub>j'</sub>は、乱数パラメータd<sub>j</sub>の初期値であり、d<sub>j'</sub> = 18である（ステップS222）。

## 【0128】

鍵サーバ220は、図17に示すように、ID受信部221、鍵再生成部22

2、公開鍵送信部223及び秘密鍵送信部224から構成される。

#### 【0129】

ID受信部221は、受信装置230から電話回線260を介して、受信装置230の固有番号ID<sub>j</sub>（1≤j≤n）を受信すると、受信した固有番号ID<sub>j</sub>を鍵再生成部222に出力する。

#### 【0130】

鍵再生成部222は、ID受信部221から固有番号ID<sub>j</sub>を受け取ると、NTTR暗号方式の秘密鍵多項式f<sub>j'</sub>と公開鍵多項式h<sub>j'</sub>を生成し、受け取った固有番号ID<sub>j</sub>と生成した公開鍵多項式h<sub>j'</sub>を公開鍵送信部223に出力し、生成した秘密鍵多項式f<sub>j'</sub>を秘密鍵送信部224に出力する。

#### 【0131】

公開鍵送信部223は、鍵再生成部222から固有番号ID<sub>j</sub>と公開鍵多項式h<sub>j'</sub>を受け取ると、受け取った固有番号ID<sub>j</sub>と公開鍵多項式h<sub>j'</sub>を、専用回線250を介してコンテンツサーバ210へ送信する。

#### 【0132】

秘密鍵送信部224は、鍵再生成部222から秘密鍵多項式f<sub>j'</sub>を受け取ると、受け取った秘密鍵多項式f<sub>j'</sub>を、電話回線260を介して受信装置230へ送信する。

#### 【0133】

以上に述べた鍵サーバ220の動作について、図18に示すフローチャートを用いて説明する。

#### 【0134】

ID受信部221は、受信装置230から電話回線260を介して、受信装置230の固有番号ID<sub>j</sub>（1≤j≤n）を受信したら、ステップS232へ処理を移し、そうでなければ処理を終了する（ステップS231）。ID受信部221は、受信した固有番号ID<sub>j</sub>を鍵再生成部222に出力する（ステップS232）。

#### 【0135】

次に、鍵再生成部222は、ID受信部221から固有番号IDを受け取り、

N T R U暗号方式の秘密鍵多項式  $f_{j'}$  と公開鍵多項式  $h_{j'}$  を生成し、受け取った固有番号  $I D_j$  と生成した公開鍵多項式  $h_{j'}$  を公開鍵送信部223に出力し、生成した秘密鍵多項式  $f_{j'}$  を秘密鍵送信部224に出力する（ステップS233）。

#### 【0136】

次に、公開鍵送信部223は、鍵再生成部222から固有番号  $I D_j$  と公開鍵多項式  $h_{j'}$  を受け取り、受け取った固有番号  $I D_j$  と公開鍵多項式  $h_{j'}$  を、専用回線250を介してコンテンツサーバ210へ送信する（ステップS234）。

#### 【0137】

次に、秘密鍵送信部224は、鍵再生成部222から秘密鍵多項式  $f_{j'}$  を受け取り、受け取った秘密鍵多項式  $f_{j'}$  を、電話回線260を介して受信装置230へ送信する（ステップS235）。

#### 【0138】

受信装置230は、図19に示すように、受信部231、秘密鍵記憶部232、復号化部233、出力部234、鍵更新用送受信部235、及び入力部236から構成される。

#### 【0139】

受信部231は、コンテンツサーバ210からインターネット240を介して、暗号化暗号鍵多項式  $E K P_i$  ( $1 \leq i \leq k$ ) と暗号化コンテンツ  $E C_i$  ( $1 \leq i \leq k$ ) を受信し、受信した暗号化暗号鍵多項式  $E K P_i$  ( $1 \leq i \leq k$ ) と暗号化コンテンツ  $E C_i$  ( $1 \leq i \leq k$ ) を復号化部233へ出力する。

#### 【0140】

秘密鍵記憶部232は、受信装置320の秘密鍵多項式  $f_{j'}$  を記憶している。

#### 【0141】

復号化部233は、暗号化部217が有する暗号アルゴリズムEの逆変換である、N T R U暗号方式の復号アルゴリズムDと、暗号化部217が有する共通鍵暗号アルゴリズム  $S y m$  を予め有している。

#### 【0142】

復号化部233は、受信部231から暗号化暗号鍵多項式EKP<sub>i</sub>（ $1 \leq i \leq k$ ）と暗号化コンテンツEC<sub>i</sub>（ $1 \leq i \leq k$ ）を受け取り、秘密鍵記憶部232から受信装置230の秘密鍵多項式f<sub>j</sub>を読み出す。そして、復号化部233は、秘密鍵多項式f<sub>j</sub>を用いて、暗号化暗号鍵多項式EKP<sub>i</sub>（ $1 \leq i \leq k$ ）に前記復号アルゴリズムDを施して、復号暗号鍵多項式KP<sub>i'</sub> = D(EKP<sub>i</sub>, f<sub>j</sub>)（ $1 \leq i \leq k$ ）を生成する。

#### 【0143】

そして、復号化部233は、コンテンツサーバ210の暗号化部217における変換の逆変換を用いて、復号暗号鍵多項式KP<sub>i</sub>（ $1 \leq i \leq k$ ）を復号暗号鍵K<sub>i</sub>（ $1 \leq i \leq k$ ）に変換する。

#### 【0144】

そして、復号化部233は、復号暗号鍵K<sub>i'</sub>（ $1 \leq i \leq k$ ）を使用して、暗号化コンテンツEC<sub>i</sub>（ $1 \leq i \leq k$ ）に共通鍵暗号アルゴリズムSymを施して、復号コンテンツCNT<sub>i'</sub> = Sym(EC<sub>i</sub>, K<sub>i'</sub>)（ $1 \leq i \leq k$ ）を生成し、復号コンテンツCNT<sub>i'</sub>（ $1 \leq i \leq k$ ）を出力部234に出力する。

#### 【0145】

出力部234は、例えばモニタやスピーカ等を備えており、入力された復号コンテンツCNT<sub>i'</sub>（ $1 \leq i \leq k$ ）を外部に出力する。

#### 【0146】

モニタは、復号コンテンツCNT<sub>i'</sub>（ $1 \leq i \leq k$ ）のMPEG2データから得られる映像を外部に出力し、スピーカ335は、復号コンテンツCNT<sub>i'</sub>（ $1 \leq i \leq k$ ）のMPEG2データから得られる音声を外部に出力する。

#### 【0147】

鍵更新用送受信部235は、入力部236を介して鍵再生成要求信号を受け取った場合、受信装置230の固有番号ID<sub>j</sub>を、電話回線260を介して鍵サーバ220へ送信し、鍵サーバ220から電話回線260を介して、秘密鍵多項式f<sub>j'</sub>を受信して、秘密鍵記憶部232に記憶されている秘密鍵多項式f<sub>j</sub>を受信した秘密鍵多項式f<sub>j'</sub>に更新する。

#### 【0148】

受信装置230を扱うユーザjは、受信装置230の公開鍵多項式 $h_j$ と秘密鍵多項式 $f_j$ の再生成を指示する鍵再生成要求信号を入力部335に入力することができる。この鍵再生成要求信号は、出力部234から出力された復号コンテンツ $CNT_i'$  ( $1 \leq i \leq k$ ) が正しく得られない等の理由で、ユーザが公開鍵多項式 $h_j$ と秘密鍵多項式 $f_j$ の再生成のために入力する信号である。

## 【0149】

入力部236は、外部から入力された鍵再生成要求信号を鍵更新用送受信部235に出力する。

## 【0150】

以上に述べた受信装置230は、以下に述べる復号化処理及び鍵更新処理を並行して非同期的に行う（処理の順番は問わない）。

## 【0151】

以下に、受信装置230の動作について、復号化処理、鍵更新処理に分けて説明を行う。

## 【0152】

最初に、受信装置230の復号化処理について、図20に示すフローチャートを用いて説明する。

## 【0153】

まず、受信部231は、コンテンツサーバ210からインターネット240を介して、暗号化暗号鍵多項式 $EKP_i$  ( $1 \leq i \leq k$ ) と暗号化コンテンツ $EC_i$  ( $1 \leq i \leq k$ ) を受信し、受信した暗号化暗号鍵多項式 $EKP_i$  ( $1 \leq i \leq k$ ) と暗号化コンテンツ $EC_i$  ( $1 \leq i \leq k$ ) を復号化部233へ出力する（ステップS251）。

## 【0154】

次に、復号化部233は、受信部231から暗号化暗号鍵多項式 $EKP_i$  ( $1 \leq i \leq k$ ) と暗号化コンテンツ $EC_i$  ( $1 \leq i \leq k$ ) を受け取り、秘密鍵記憶部232から受信装置230の秘密鍵多項式 $f_j$ を読み出し（ステップS252）、そして、秘密鍵多項式 $f_j$ を用いて、暗号化暗号鍵多項式 $EKP_i$  ( $1 \leq i \leq k$ ) に復号アルゴリズムDを施して、復号暗号鍵多項式 $KP_i' = D(EKP_i)$

,  $f_{j'}$ ) ( $1 \leq i \leq k$ ) を生成する (ステップ S 253)。

#### 【0155】

次に、復号化部 233 は、コンテンツサーバ 210 の暗号化部 217 における変換の逆変換を用いて、復号暗号鍵多項式  $K_{P_i}$  ( $1 \leq i \leq k$ ) を復号暗号鍵  $K_i$  ( $1 \leq i \leq k$ ) に変換する (ステップ S 254)。

#### 【0156】

次に、復号化部 233 は、復号暗号鍵  $K_{i'}$  ( $1 \leq i \leq k$ ) を使用して、暗号化コンテンツ  $EC_i$  ( $1 \leq i \leq k$ ) に共通鍵暗号アルゴリズム Sym を施して、復号コンテンツ  $CNT_{i'} = Sym(EC_i, K_{i'})$  ( $1 \leq i \leq k$ ) を生成し、復号コンテンツ  $CNT_{i'}$  ( $1 \leq i \leq k$ ) を出力部 234 に出力する (ステップ S 255)。

#### 【0157】

次に、出力部 234 は、それぞれ、復号コンテンツ  $CNT_{i'}$  ( $1 \leq i \leq k$ ) のMPEG2データから得られる映像及び音声を外部に出力して処理を終了する (ステップ S 256)。

#### 【0158】

次に、受信装置 230 の鍵更新処理について、図 21 に示すフローチャートを用いて説明する。

#### 【0159】

まず、鍵更新用送受信部 235 は、もしも、入力部 236 を介して鍵再生成要求信号を受け取ったら、ステップ S 262 へ処理を移し、そうでなければ処理を終了する (ステップ S 261)。

#### 【0160】

次に、鍵更新用送受信部 235 は、受信装置 230 の固有番号 ID<sub>j</sub> を、電話回線 260 を介して鍵サーバ 220 へ送信し (ステップ S 262)、鍵サーバ 220 から電話回線 260 を介して、秘密鍵多項式  $f_{j'}$  を受信して、秘密鍵記憶部 232 に記憶されている秘密鍵多項式  $f_j$  を受信した秘密鍵多項式  $f_{j'}$  に更新して処理を終了する (ステップ S 263)。

#### 【0161】

以下に、実施の形態2における暗号システム2全体の動作について暗号システム1との差異点を中心に説明する。

#### 【0162】

まず、コンテンツサーバ210は、受信装置230の固有番号IDj、公開鍵多項式 $h_j$ 及び乱数パラメータ $d_j$ を、データDTj = (IDj, hj, dj)としてパラメータ記憶部212に記憶している。乱数パラメータdjの初期値は、 $d_j = 18$ である。

#### 【0163】

そして、コンテンツサーバ210は暗号化通信処理に従って、コンテンツCN<sub>Ti</sub> ( $1 \leq i \leq k$ )を暗号鍵K<sub>i</sub> ( $1 \leq i \leq k$ )を用いて共通鍵暗号で暗号化して暗号化コンテンツEC<sub>i</sub> ( $1 \leq i \leq k$ )を生成し、その暗号鍵K<sub>i</sub> ( $1 \leq i \leq k$ )から変換した暗号鍵多項式KP<sub>i</sub> ( $1 \leq i \leq k$ )をNTRU暗号で暗号化して暗号化暗号鍵多項式EKP<sub>i</sub> ( $1 \leq i \leq k$ )を生成し、暗号化コンテンツEC<sub>i</sub> ( $1 \leq i \leq k$ )を暗号化暗号鍵多項式EKP<sub>i</sub> ( $1 \leq i \leq k$ )と共にインターネット240を介して受信装置230に送信する。一方、受信装置230は復号化処理に従って、暗号化コンテンツEC<sub>i</sub> ( $1 \leq i \leq k$ )と暗号化暗号鍵EK<sub>i</sub> ( $1 \leq i \leq k$ )をインターネット240を介して送信装置210から受信し、受信した暗号化暗号鍵多項式EKP<sub>i</sub> ( $1 \leq i \leq k$ )を復号して復号暗号鍵多項式KP<sub>i'</sub> ( $1 \leq i \leq k$ )を生成し、これを変換した復号暗号鍵K<sub>i</sub> ( $1 \leq i \leq k$ )を用いて、暗号化コンテンツEC<sub>i</sub> ( $1 \leq i \leq k$ )を復号して復号コンテンツCNT<sub>i'</sub> ( $1 \leq i \leq k$ )を出力する。

#### 【0164】

なお、コンテンツサーバ210では、乱数パラメータ更新処理に従って、タイマ部213が一日毎に発生する時間信号に応じて、パラメータ制御部214は、パラメータ記憶部212に記憶された全ての乱数パラメータd<sub>j</sub> ( $1 \leq j \leq n$ )の値を1ずつ増加させる。すなわち、パラメータ記憶部212に記憶された全ての乱数パラメータd<sub>j</sub> ( $1 \leq j \leq n$ )の値は一日毎に増加する。

#### 【0165】

従って、このコンテンツサーバ210の暗号化通信処理が継続して行われると

、暗号化暗号鍵多項式  $EKP_i$  ( $1 \leq i \leq k$ ) を生成される際に用いられる乱数多項式  $r_i$  ( $1 \leq i \leq k$ ) は、係数が 1 であるもの、及び係数が -1 であるものの数が一日毎に増加する。

#### 【0166】

今、図10は、乱数パラメータ  $d$  の値に対し、 $d$  個の係数が 1 であり、かつ  $d$  個の係数が -1 であり、かつその他の係数が 0 となる乱数多項式  $r$  を用いた場合の、NTRU暗号方式の復号エラー発生確率の測定結果である。この測定結果によれば、乱数パラメータ  $d_j$  の初期値  $d_j = 18$ においては、コンテンツサーバ210が生成する暗号化暗号鍵多項式  $EKP_i$  ( $1 \leq i \leq k$ ) は、ほとんど復号エラーは発生しない（受信装置230は受信した暗号化暗号鍵多項式  $EKP_i$  ( $1 \leq i \leq k$ ) から暗号鍵  $K_i$  と等しい復号暗号鍵  $K'_i$  を得ることができて正しくコンテンツCNT*i*が復号できる）。一方で、期間が経過すれば、乱数パラメータ  $d_j$  が一日毎に徐々に大きくなるので、コンテンツサーバ210が生成する暗号化暗号鍵多項式  $EKP_i$  ( $1 \leq i \leq k$ ) は、徐々に復号エラー発生確率が大きくなる（受信装置230は受信した暗号化暗号鍵多項式  $EKP_i$  ( $1 \leq i \leq k$ ) から暗号鍵  $K_i$  と等しい復号暗号鍵  $K'_i$  を得ることが徐々にできなくなり、コンテンツCNT*i*を徐々に正しく復号できなくなる）。

#### 【0167】

そして、もしも受信装置230がコンテンツCNT*i* ( $1 \leq i \leq k$ ) を正しく復号できる確率が下がり、実用的な暗号化通信を行うことができなくなった場合、受信装置230を扱うユーザ  $j$  は、鍵更新処理を行うことにより、受信装置230の公開鍵多項式  $h_j$  と秘密鍵多項式  $f_j$  の再生成を指示する鍵再生成要求信号を入力部236に入力することができる。すると、鍵サーバ220により、コンテンツサーバ210のパラメータ記憶部212の乱数パラメータ  $d_j$  は初期値  $d_j' = 18$  に更新されるので、復号エラー発生確率が元に戻り、再び受信装置230は実用的に暗号化通信を行うことができるようになる。

#### 【0168】

実施の形態2では、デジタルデータであるコンテンツCNTを一定時間毎に分割し、CNT*i* ( $1 \leq i \leq k$ ) を受信装置230へ配信している。一般に、MP

EG2のようなデジタルデータの場合、復号エラーが発生して正しくCNTiを得られないと、動画像や音声にノイズが発生する。従って、期間が経過すると、復号エラーの発生確率が増加し、徐々に動画像や音声にノイズが増えることになる。これにより、コンテンツを提供する業者が、例えば1ヶ月間は実用上問題ないノイズ発生レベルでコンテンツをユーザに視聴させ、1ヶ月を過ぎると復号エラー発生確率が増加してノイズ発生レベルが大きくなり、鍵更新を行わない限りユーザがコンテンツを実用的に視聴できないようにさせることができる。すなわち、期間限定のコンテンツ配信に適する。

#### 【0169】

また、一般に、MPEG2のようにサイズが大きいCNTi ( $1 \leq i \leq k$ ) の場合、各CNTiを全てNTRU暗号で暗号化しようとすると、NTRU暗号の入力ビット長に合わせてCNTiを分割し、複数回NTRU暗号の暗号処理を行わなければならない。しかし、この場合、暗号鍵KiをNTRU暗号で暗号化し、サイズの大きいコンテンツCNTiは公開鍵暗号に比べて速度の速い共通鍵暗号で暗号化するので、高速処理が可能であり、コンテンツ配信に適する。

#### 【0170】

また、鍵の更新時に、鍵サーバ220を利用するので、鍵サーバ220でユーザjの鍵更新の回数を把握することができ、この回数によりコンテンツを提供する業者がユーザjにコンテンツ配信の課金を行うこともできる。

#### 【0171】

なお、実施の形態1で得られる効果も同様に得られる。

#### 【0172】

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。以下のような場合も本発明に含まれる。

#### 【0173】

用いるNTRU暗号のパラメータはN=167に限定されず、他のパラメータでもよい。

#### 【0174】

パラメータ制御部114、214では、一日毎に乱数パラメータを1ずつ増加させる以外に、期間が経過するにつれて徐々に増加させれば、任意の期間毎に乱数パラメータを増加させてもよいし、またパラメータの増加分を任意にしてもよい。

#### 【0175】

さらに、パラメータ制御部114、214は、期間の経過に応じてではなく、乱数パラメータが読み出される毎に乱数パラメータを増加させてもよいし、乱数パラメータが読み出される回数に応じて乱数パラメータを増加させてもよい。これにより、暗号化回数が多くなるにつれ、徐々に復号エラー発生確率が大きくなるようにすることができるので、暴露された秘密鍵を有する第三者の受信装置に復号され続けることを防止でき、また受信装置又は受信装置を扱う人に鍵の更新を促すことができる。また、これにより、期間限定のコンテンツ配信以外にも、回数限定のコンテンツ配信にも利用できるようになる。

#### 【0176】

鍵再生成要求信号は入力部126、236を介して外部から入力される代わりに、受信装置120、230、が何らかの方法で復号エラーを検知して、自動的に鍵再生要求信号が入力されるようにしてもよい。

#### 【0177】

これは、例えば、実施の形態2における復号化部233が、さらに、復号コンテンツCNT<sub>i'</sub>がMPEG2のフォーマットに従っているかどうかを判別して復号エラーを検知し、復号エラー発生の度合が大きくなったら鍵再生成要求信号を入力部236に入力することで実現できる。また、例えば、平文多項式mや暗号鍵多項式KP<sub>i</sub>（ $1 \leq i \leq k$ ）の高次の10次元分の係数を1とする等、そのフォーマットを定めておき、復号化部123、223が、さらに、復号文多項式m'や復号暗号鍵多項式KP<sub>i'</sub>がそのフォーマットに従うかどうかを判別して復号エラーを検知し、復号エラー発生の度合が大きくなったら鍵再生成要求信号を入力部126、236に入力することでも実現できる。

#### 【0178】

実施の形態2において、インターネット240、専用回線250、電話回線2

60は、衛生通信網等の他の通信路を用いてもよいし、また同じ通信路を用いてもよい。なお、鍵サーバ220と受信装置230との間の通信路では、秘密鍵fjの送信が行われるので、安全性を高めるために暗号化通信を行ってもよい。

#### 【0179】

実施の形態2において、共通鍵暗号アルゴリズムSymとして、AES暗号等の他の共通鍵暗号方式を用いてもよい。

#### 【0180】

実施の形態2において、コンテンツCNTi ( $1 \leq i \leq k$ ) は、MPEG2データに限らず、Windows (R) Media PlayerやRealPlayerで再生可能なデジタルデータでもよいし、そのデータの形式は限られない。

#### 【0181】

実施の形態2において、コンテンツサーバ210と鍵サーバ320は同一システム内にあってもよい。

#### 【0182】

本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

#### 【0183】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピュータ読み取り可能な記録媒体、例えば、半導体メモリ、ハードディスクドライブ、CD-ROM、DVD-ROM, DVD-RAM等、に記録したものとしてもよい。

#### 【0184】

上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

#### 【0185】

##### 【発明の効果】

以上に説明したように、本発明は、従来システムにおける問題点を鑑みて行われたもので、暗号システムにおいて、暗号化通信にNTRU暗号方式を用い、送

信装置で乱数パラメータを期間が経過するにつれ増加させるようにしたので、期間が経過するにつれて、受信装置で暗号化通信を正しく復号できなくなるようにすることが可能となった。

#### 【0186】

これにより、送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム又は送信装置を提供でき、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容が、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することが可能となった。

#### 【0187】

また、送信装置が暗号化通信を行うに際して、正規の受信者の受信装置は、復号を行うに従い、復号に失敗する確率が徐々に増大する暗号システム、送信装置又は受信装置を提供し、これにより受信装置又は受信装置を扱う人に、鍵の更新を促すようにすることが可能となった。

#### 【0188】

さらに、送信装置が暗号化通信を行うに際して、第三者機関によるCRLやSRMを必要としない暗号システム、送信装置又は受信装置を提供することが可能となった。

#### 【0189】

以上により、従来技術では達成できなかった暗号システムを提供することができ、その価値は大きい。

#### 【図面の簡単な説明】

##### 【図1】

本発明の実施の形態1における暗号システム1の構成を示す図

##### 【図2】

本発明の実施の形態1における送信装置110の構成を示す図

##### 【図3】

本発明の実施の形態1におけるパラメータ記憶部112の構成を示す図

##### 【図4】

本発明の実施の形態1における送信装置110の暗号化通信処理の流れを示すフローチャート

【図5】

本発明の実施の形態1における送信装置110の乱数パラメータ更新処理の流れを示すフローチャート

【図6】

本発明の実施の形態1における送信装置110の公開鍵更新処理の流れを示すフローチャート

【図7】

本発明の実施の形態1における受信装置120aの構成を示す図

【図8】

本発明の実施の形態1における受信装置120aの復号化処理の流れを示すフローチャート

【図9】

本発明の実施の形態1における受信装置120aの鍵更新処理の流れを示すフローチャート

【図10】

NTRU暗号方式の復号エラー発生確率の測定結果を示す図

【図11】

本発明の実施の形態2における暗号システム2の構成を示す図

【図12】

本発明の実施の形態2におけるコンテンツサーバ210の構成を示す図

【図13】

本発明の実施の形態2におけるパラメータ記憶部212の構成を示す図

【図14】

本発明の実施の形態2におけるコンテンツサーバ210の暗号化通信処理の流れを示すフローチャート

【図15】

本発明の実施の形態2におけるコンテンツサーバ210の乱数パラメータ更新

処理の流れを示すフローチャート

【図16】

本発明の実施の形態2におけるコンテンツサーバ210の公開鍵更新処理の流れを示すフローチャート

【図17】

本発明の実施の形態2における鍵サーバ220の構成を示す図

【図18】

本発明の実施の形態2における鍵サーバ220の処理の流れを示すフローチャート

【図19】

本発明の実施の形態2における受信装置230の構成を示す図

【図20】

本発明の実施の形態2における受信装置230の復号化処理の流れを示すフローチャート

【図21】

本発明の実施の形態2における受信装置230の鍵更新処理の流れを示すフローチャート

【符号の説明】

1, 2 暗号システム

110 送信装置

111 平文入力部

112, 212 パラメータ記憶部

113, 213 タイマ部

114, 214 パラメータ制御部

115, 215 乱数生成部

116, 217 暗号化部

117, 218 送信部

118, 219 鍵更新部

120a, 120b, 120c, 230 受信装置

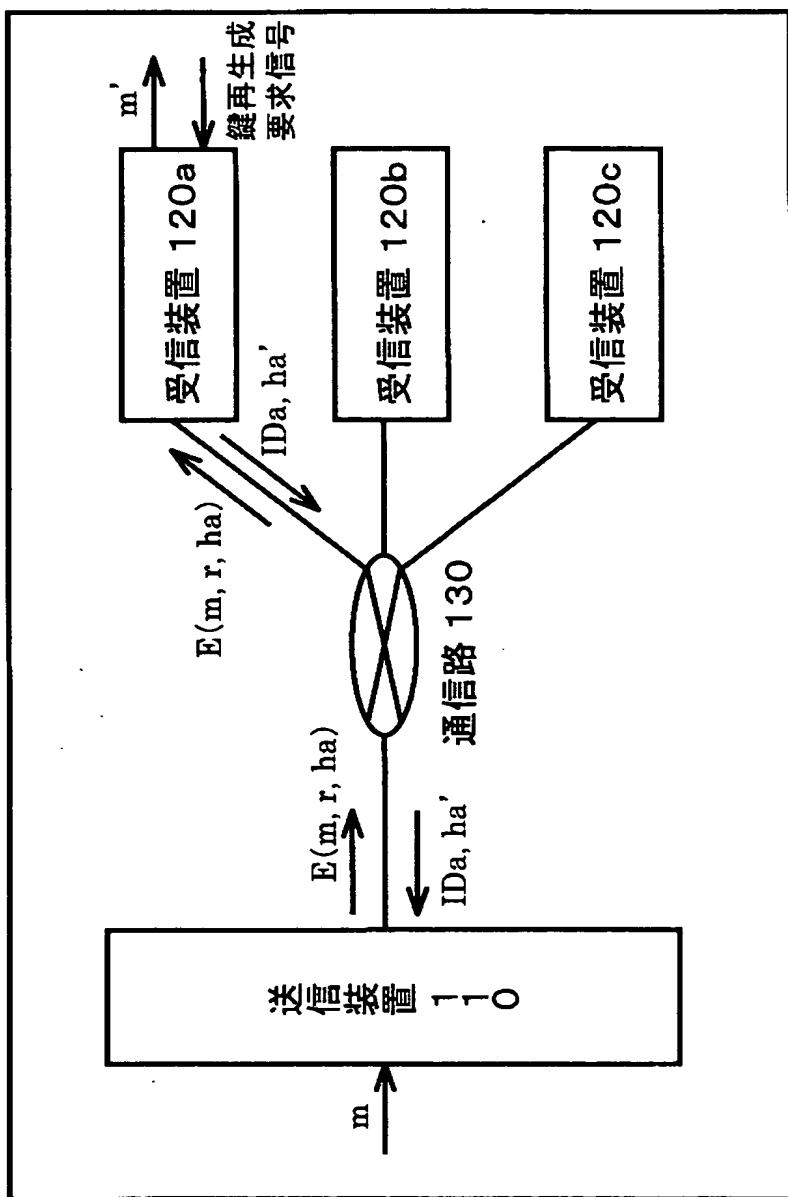
121, 231 受信部  
122, 232 秘密鍵記憶部  
123, 233 復号化部  
124 復号文出力部  
125, 222 鍵再生成部  
126, 236 入力部  
130 通信路  
210 コンテンツサーバ  
211 コンテンツ記憶部  
216 暗号鍵生成部  
220 鍵サーバ  
221 I D受信部  
223 公開鍵送信部  
224 秘密鍵送信部  
234 出力部  
235 鍵更新用送受信部  
240 インターネット  
250 専用回線  
260 電話回線

【書類名】

図面

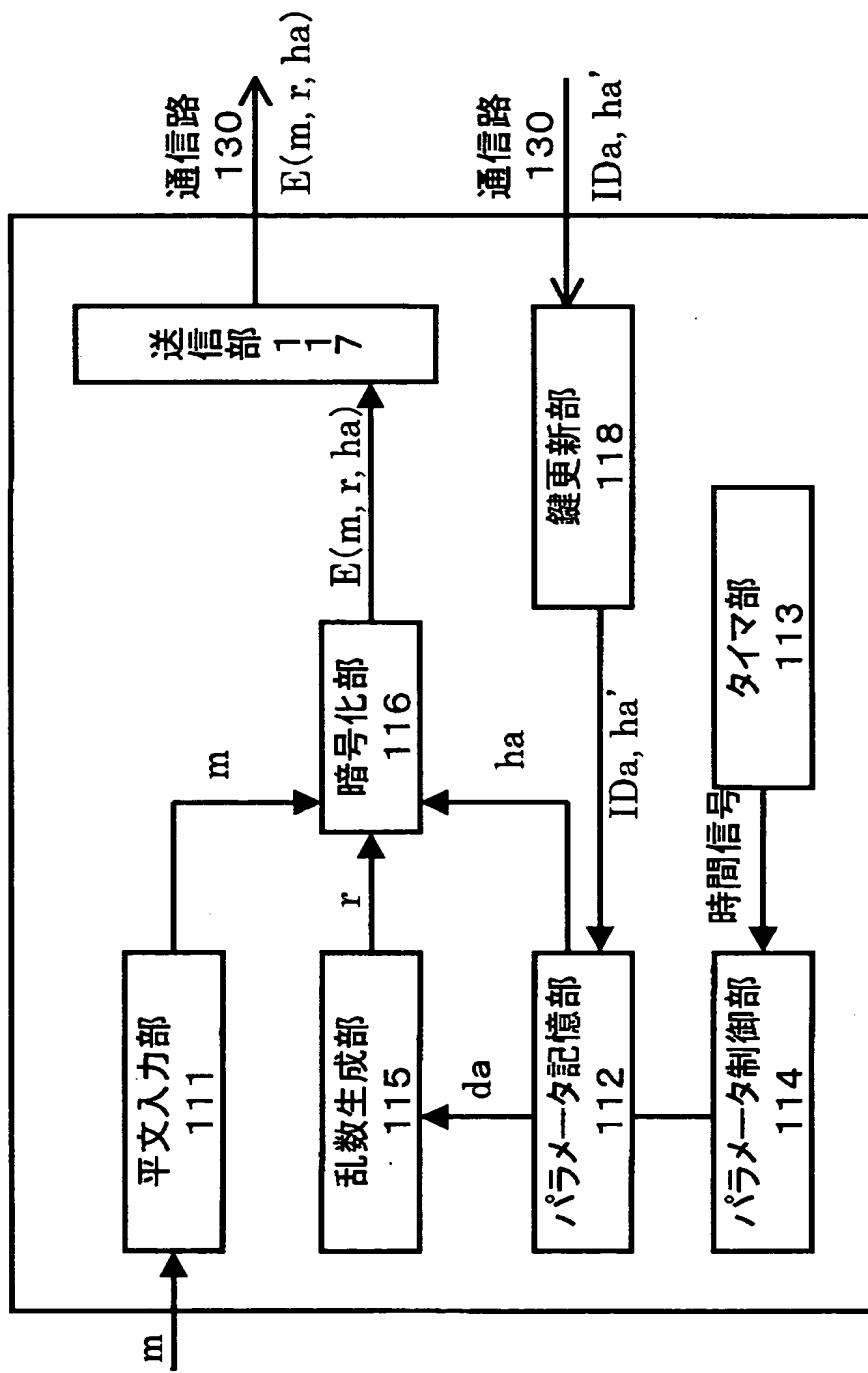
暗号システム 1

【図1】



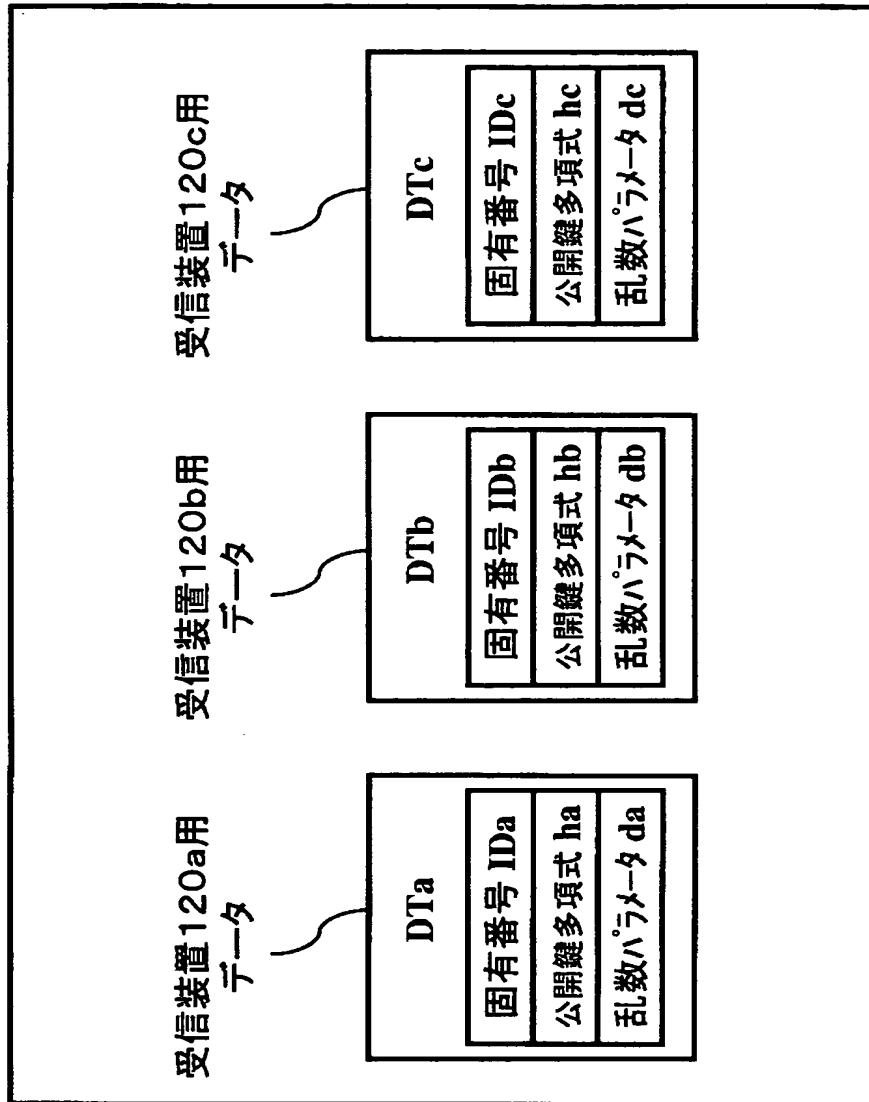
【図2】

送信装置 110

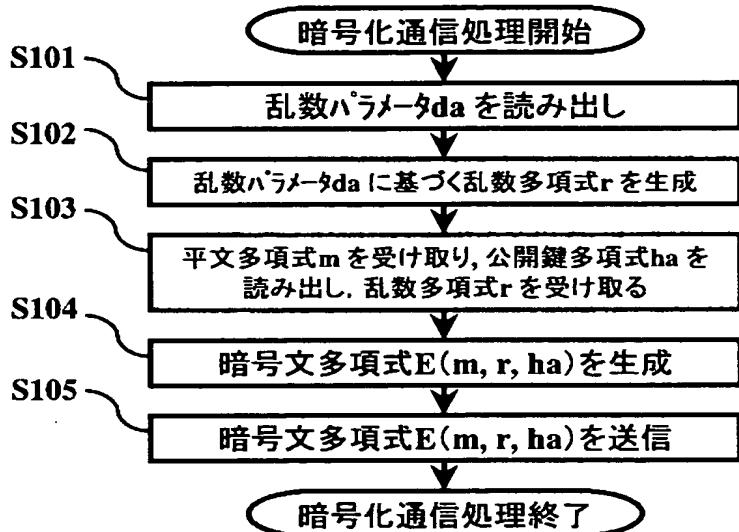


【図3】

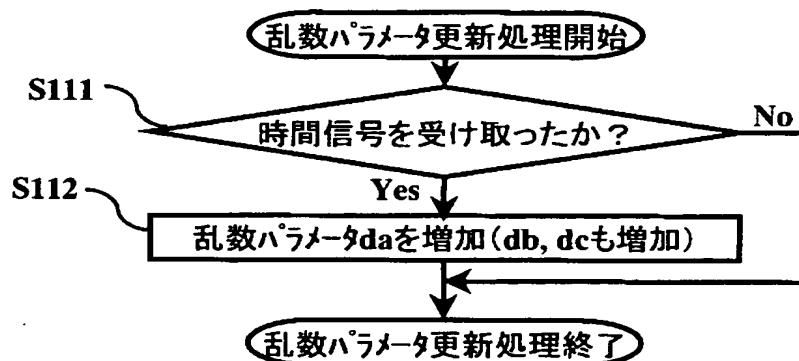
パラメータ記憶部112



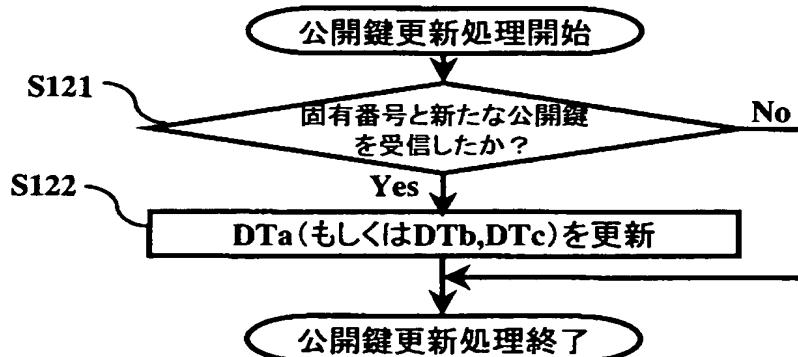
【図4】



【図5】

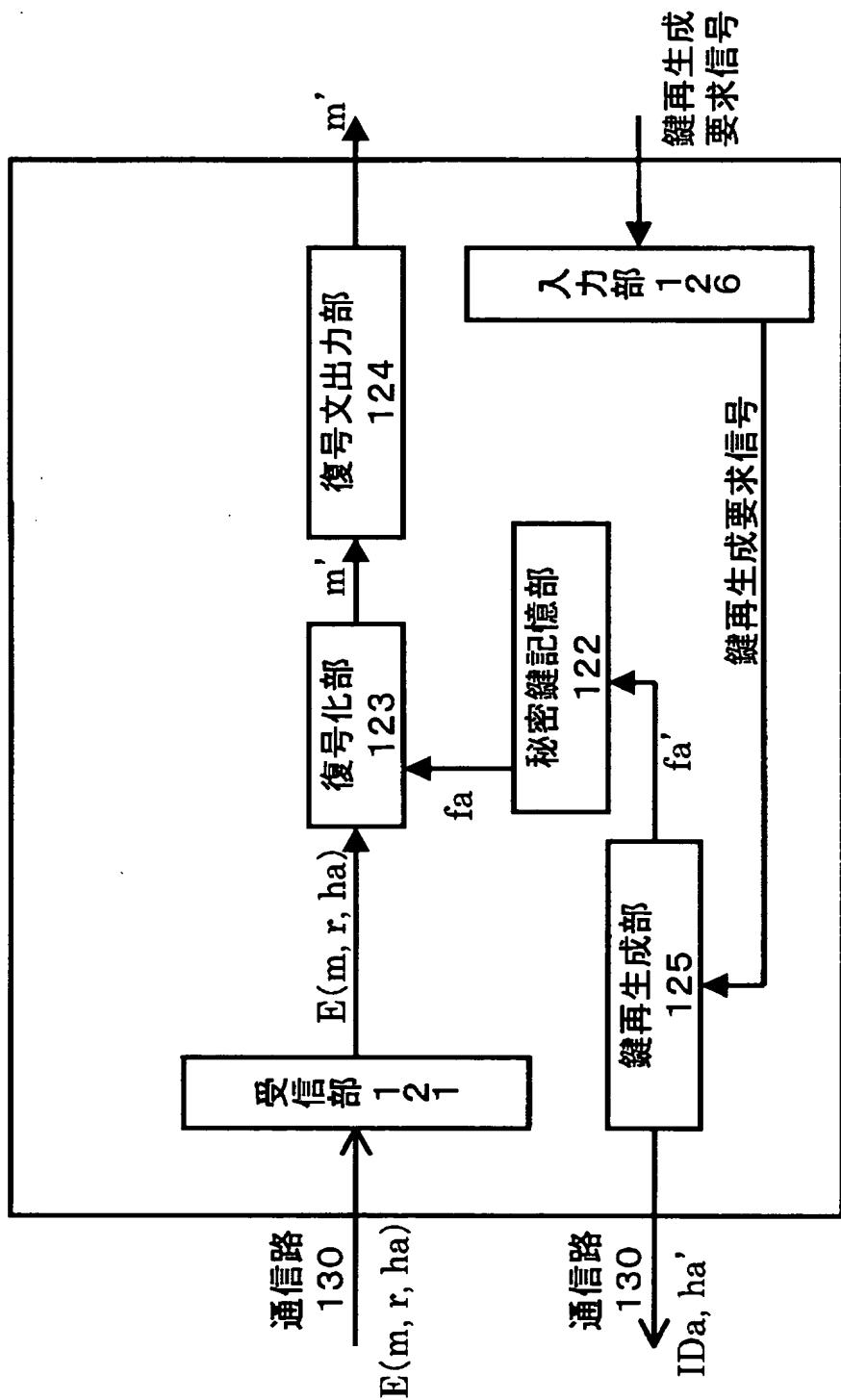


【図6】

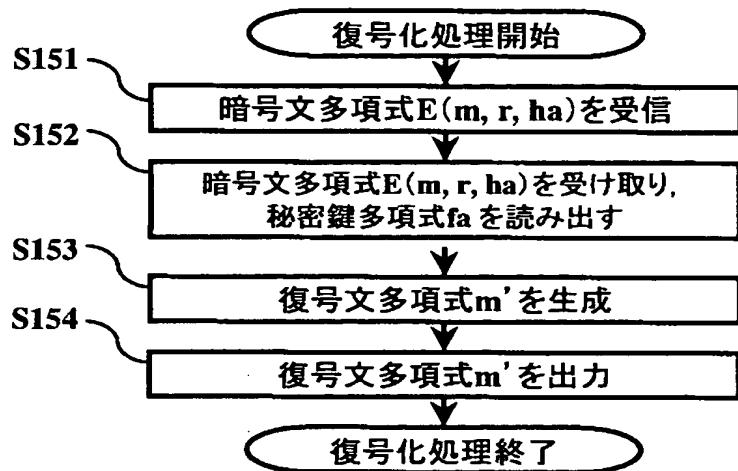


【図7】

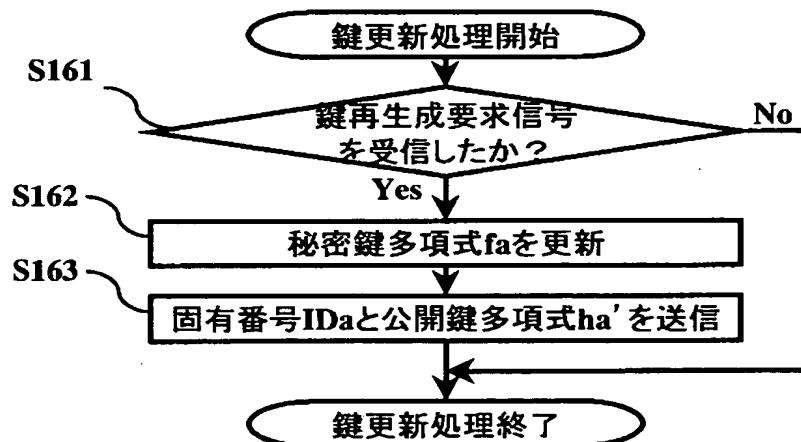
受信装置 120a



【図8】



【図9】

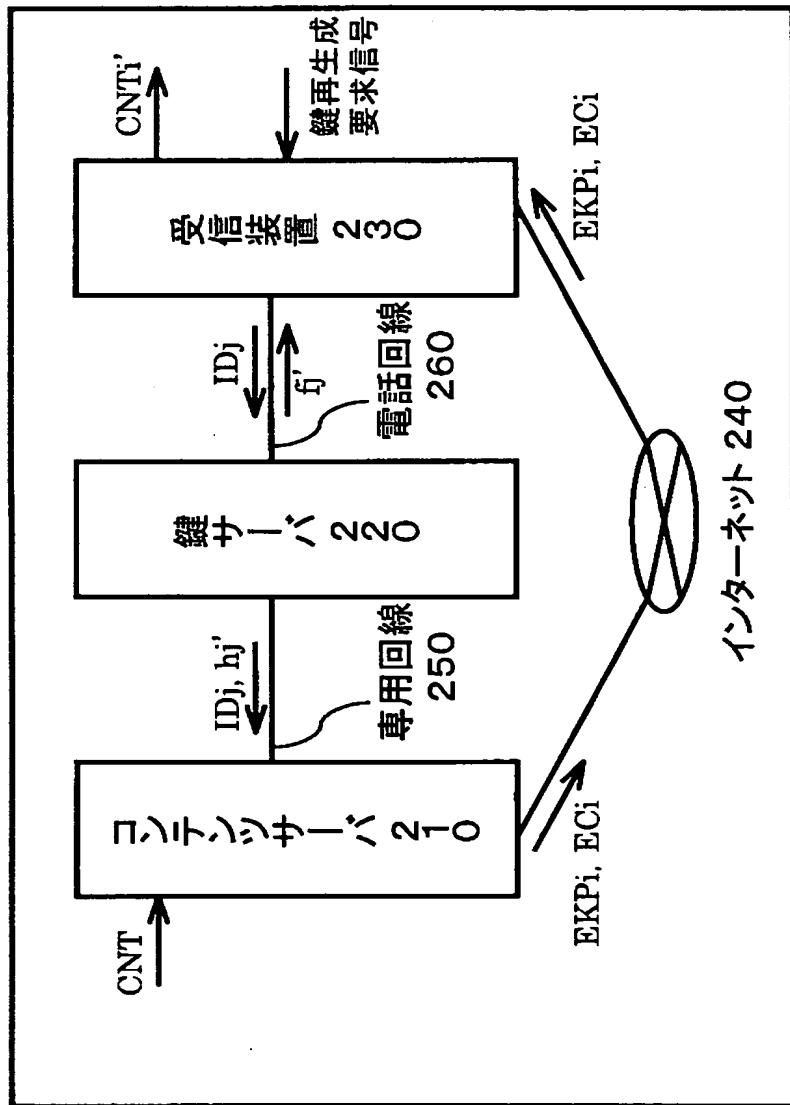


【図10】

|             |        |      |     |     |     |      |      |
|-------------|--------|------|-----|-----|-----|------|------|
| 乱数パラメータd    | 18     | 28   | 38  | 48  | 58  | 68   | 78   |
| 復号エラー発生率(%) | 0.0007 | 0.09 | 2.6 | 2.3 | 7.1 | 13.7 | 24.8 |

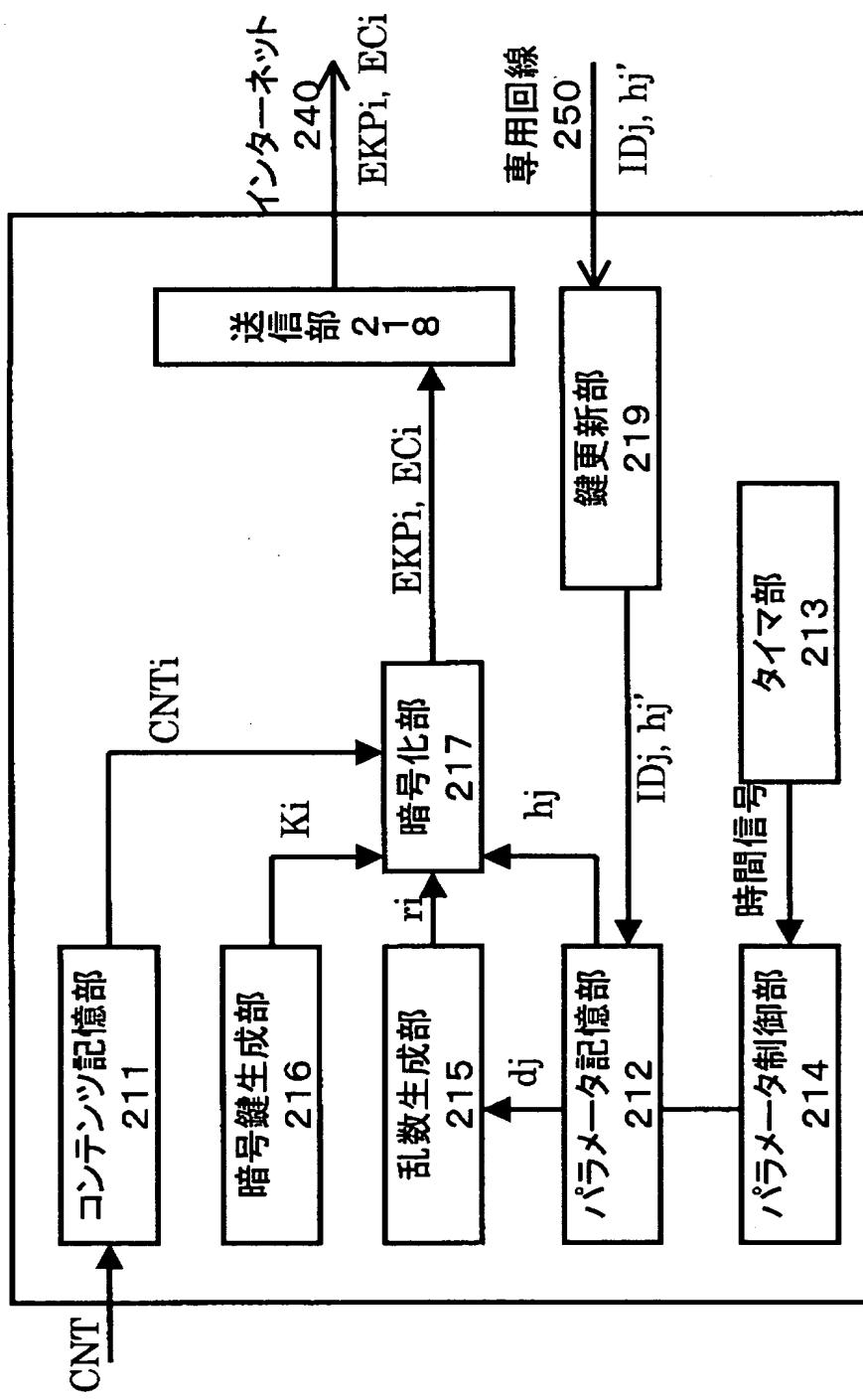
【図11】

## 暗号システム2



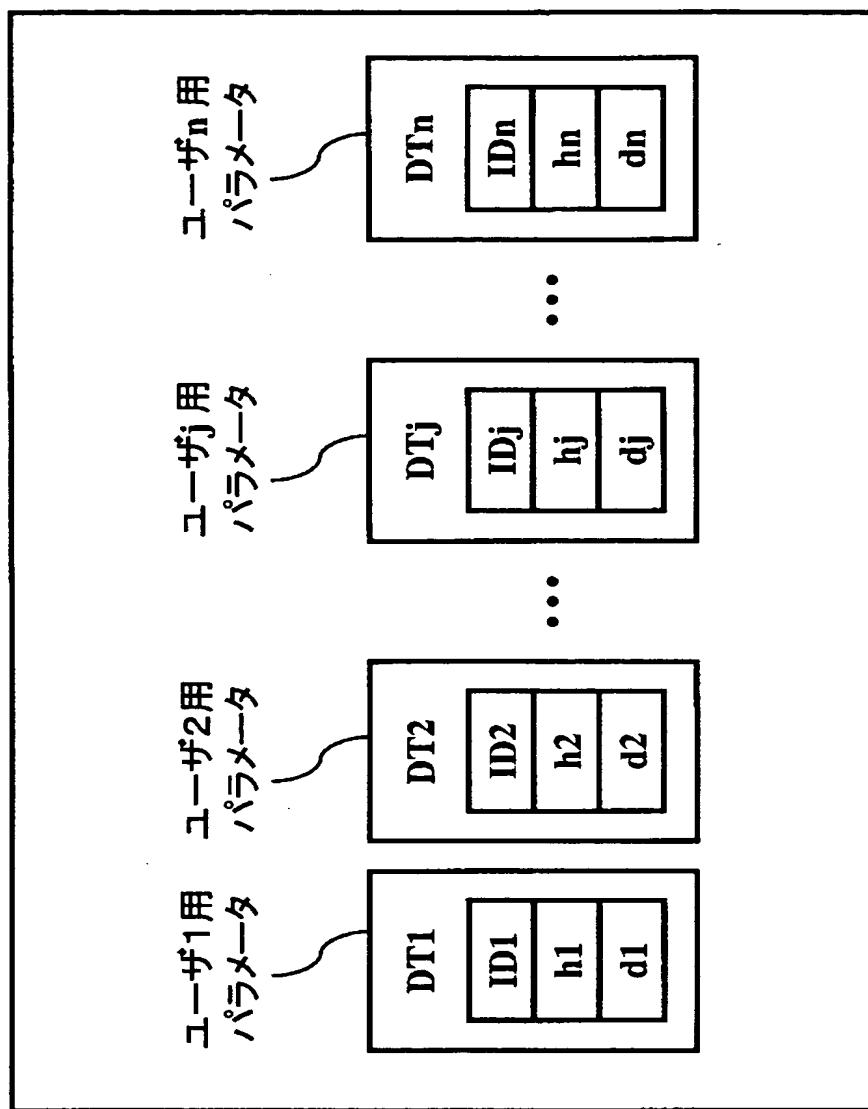
【図12】

コンテナシッサーバ210

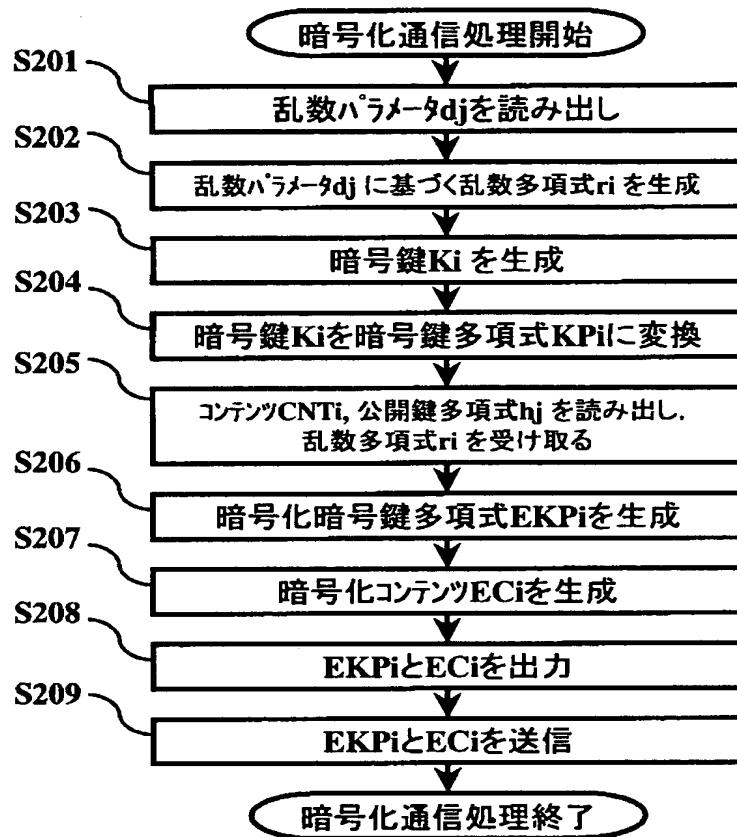


## パラメータ記憶部 212

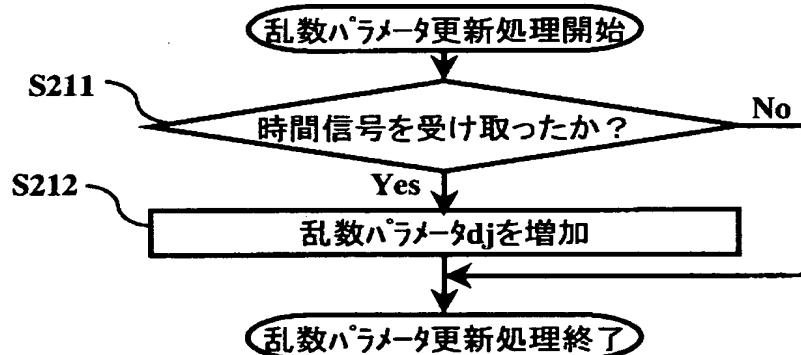
【図13】



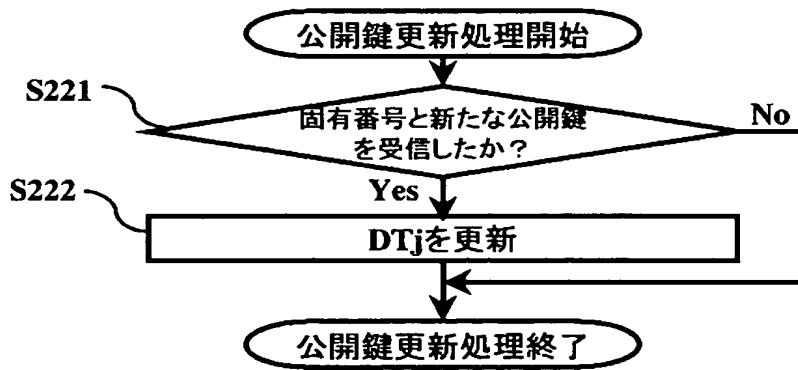
【図14】



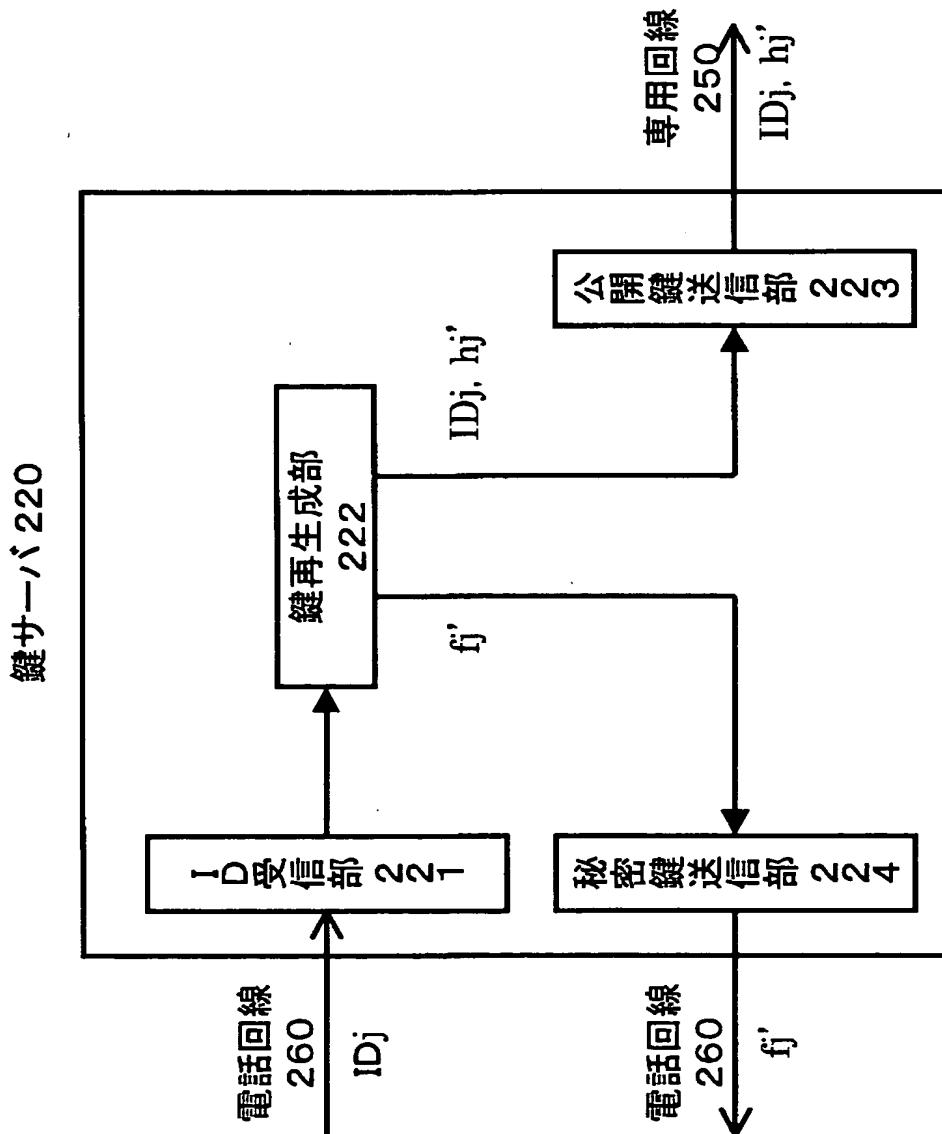
【図15】



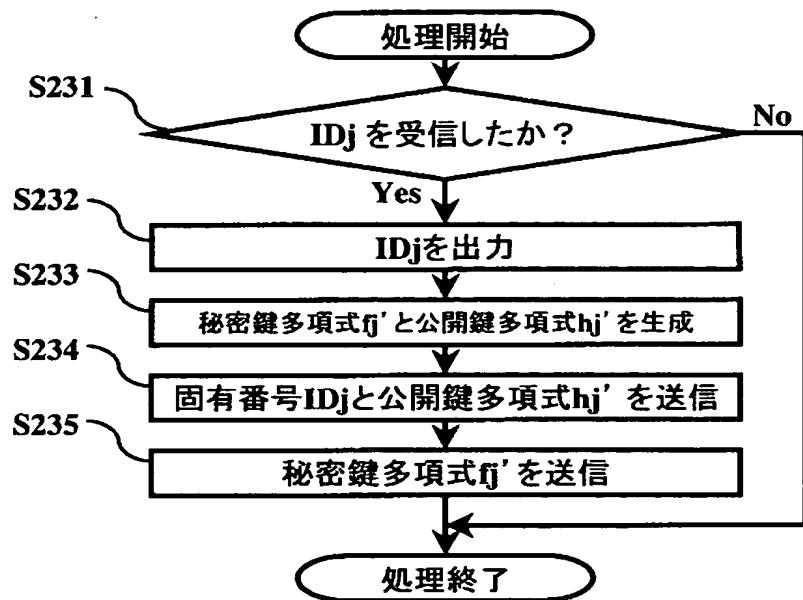
【図16】



【図17】

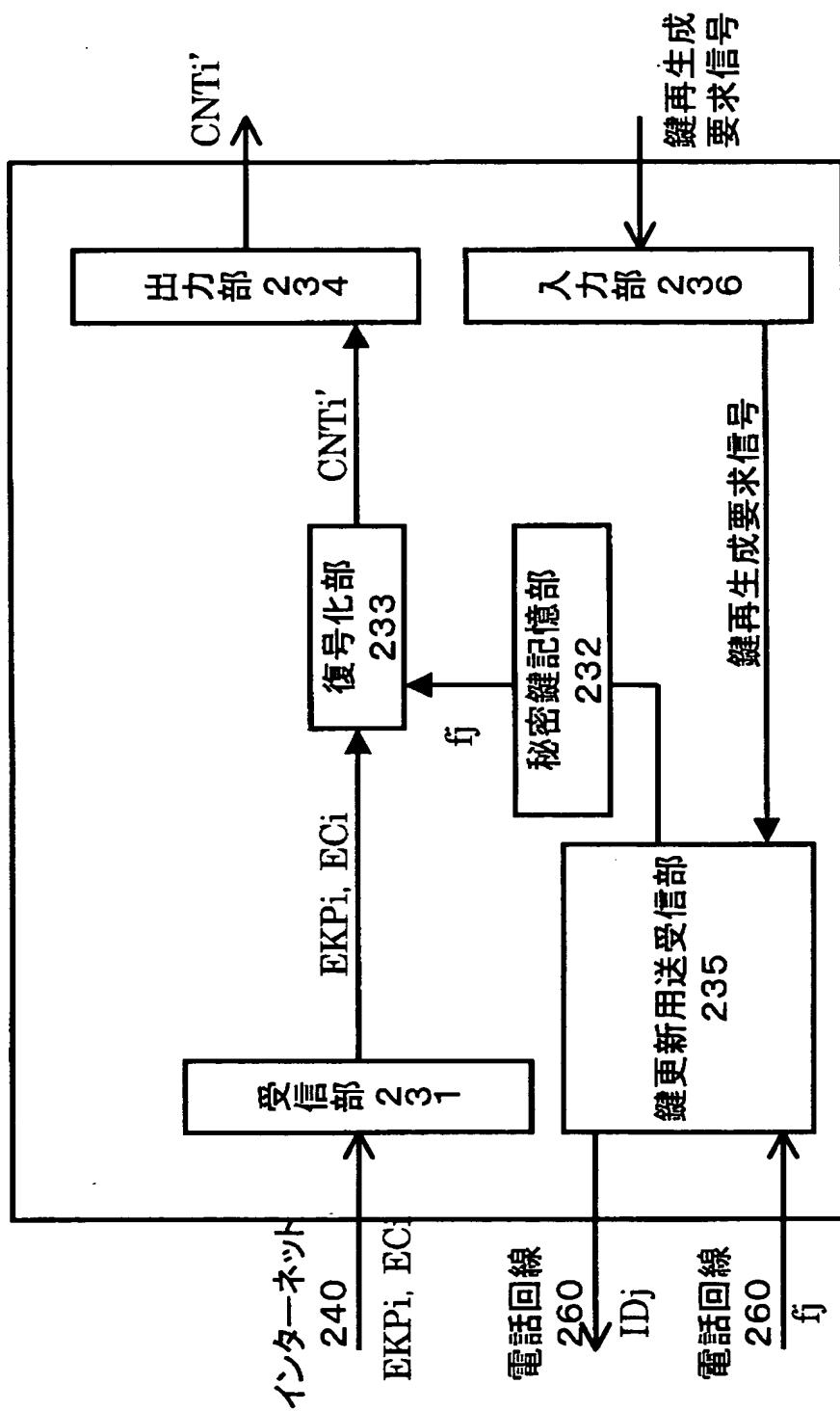


【図18】

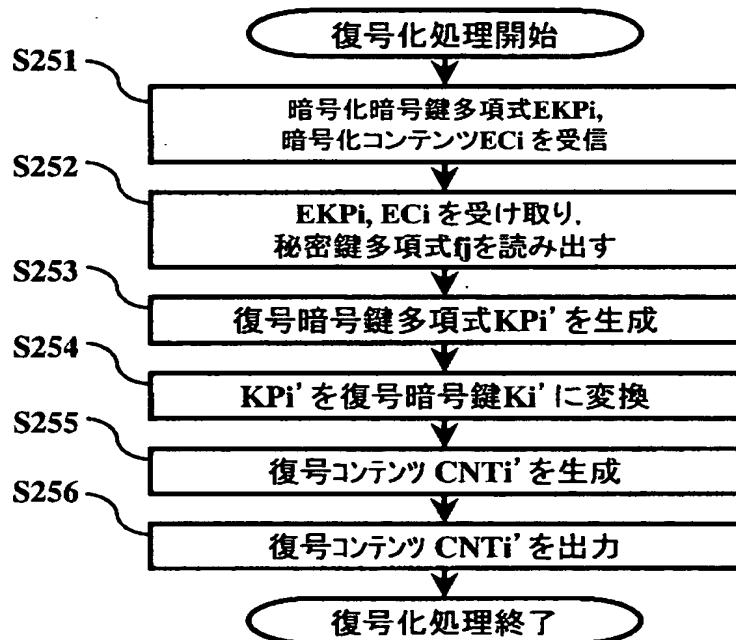


【図19】

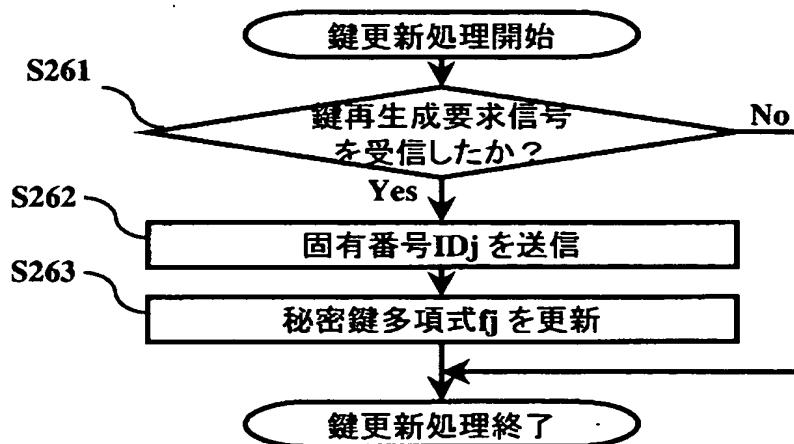
受信装置 230



【図20】



【図21】



【書類名】 要約書

【要約】

【課題】 送信装置が暗号化通信を行うに際して、暴露された秘密鍵を不正に用いる第三者の受信装置は、期間が経過すると暗号化通信が復号できなくなる暗号化システム、送信装置又は受信装置を提供し、これにより秘密鍵が暴露された場合に、送信装置が行う暗号化通信の内容を、暴露された秘密鍵を有する第三者の受信装置に復号され続けるのを防止することを第1の目的とする。

【解決手段】 本発明は、外部から入力された平文を暗号鍵で暗号化した暗号文を受信装置へ送信する送信装置が、前記受信装置毎に乱数パラメータを記憶する記憶手段と、前記平文から、前記記憶手段に記憶された前記乱数パラメータを用いて前記暗号文を生成する暗号手段と、前記記憶手段に記憶された前記乱数パラメータを制御する制御手段とを備えることを特徴とする。

【選択図】 図2

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地  
氏 名 松下電器産業株式会社